PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-048076
(43)Date of publication of application : 18.02.2000

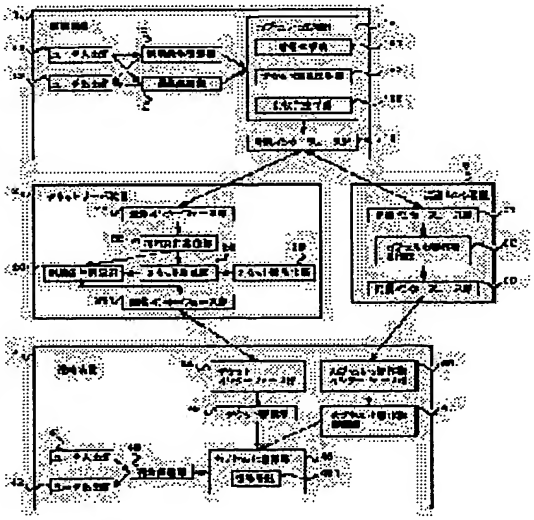
(51)Int.Cl. G06F 17/60
G06F 9/06
G06F 12/14
G06F 13/00
G06F 15/00
H04L 9/08
H04L 9/32

(21)Application number : 10-213789
(22)Date of filing : 29.07.1998

(71)Applicant : NEC CORP
(72)Inventor : NAKAE MASAYUKI

(54) SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL BOOK, DEVICE AND METHOD FOR REPRODUCING DIGITAL BOOK AND RECORD MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To describe detailed and flexible using conditions at the time of distributing a digital book and to realize the safety of the digital book.
SOLUTION: An edition device 1 capsules the using condition of each using method and utilization secret information obtained by reciphering a deciphering key for ciphered book data by a ticket key different in each using method together with the ciphered book data. A ticket server device 2 manages the using condition and the ticket key, and at the time of permitting the using method to a using request from a user issues a ticket having the ticket key. A distribution center device 3 manages the capsuled book and distributes the capsuled book in accordance with a request from a user. An observing/listening device 4 acquires the capsuled book from the device 3 and requests the ticket for the using method to the device 2. Only when the ticket is acquired the device 4 restores and reproduces the ciphered book data included in the capsuled book.



LEGAL STATUS

[Date of request for examination]	29.07.1998
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3216607
[Date of registration]	03.08.2001

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－48076
（P2000－48076A）
(43)公開日　平成12年２月18日(2000.2.18)

(51)Int.Cl.⁷	識別記号	FI		テーマコード（参考）
G06F 17/60		G06F 15/21	Z	
9/06	550		550Z	
12/14	320		320B	
13/00	351		351G	
15/00	330		330Z	

審査請求 有　請求項の数19　ＯＬ　（全 28 頁）　最終頁に続く

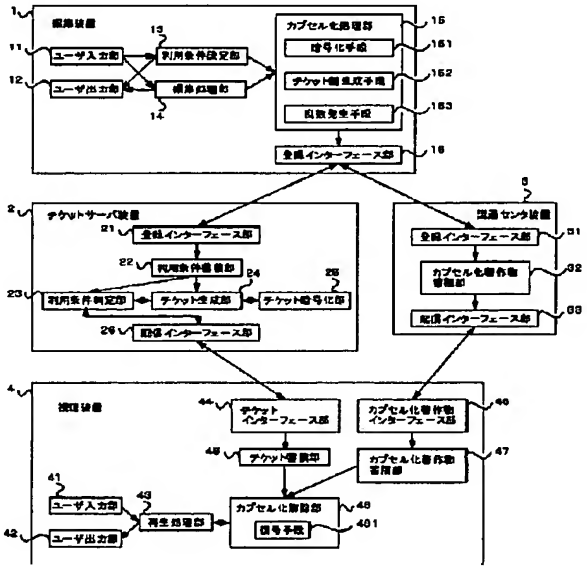
(21)出願番号　特願平10－213789

(22)出願日　平成10年７月29日(1998.7.29)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　中江　政行
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100104916
弁理士　古溝　聡　（外１名）

(54)【発明の名称】　デジタル著作物流通システム及び方法、デジタル著作物再生装置及び方法、並びに記録媒体

(57)【要約】
【課題】　デジタル著作物の流通に際して、詳細かつ柔軟な利用条件記述を行い、また、デジタル著作物の安全性を実現する。
【解決手段】　編集装置１は、利用法ごとの利用条件と、暗号化著作物データの復号鍵を利用法ごとに異なるチケット鍵により再暗号化した利用秘密情報とを、当該暗号化著作物データとともにカプセル化する。チケットサーバ装置２は、前記利用条件およびチケット鍵を管理し、利用者からの利用要求に対して利用法を許可した場合、前記チケット鍵を有したチケットを発行する。流通センタ装置３は、前記カプセル化著作物を管理し、利用者からの要求に応じてカプセル化著作物を配送する。視聴装置４は、流通センタ装置３からカプセル化著作物を取得し、その利用法に対するチケットをチケットサーバ装置２に要求する。視聴装置４は、当該チケットが取得された場合にのみ、前記カプセル化著作物に含まれる暗号化著作物データを復元し、再生する。



1

【特許請求の範囲】

【請求項１】配布すべき著作物データに利用条件を設定する利用条件設定手段と、

前記著作物データを所定の暗号鍵により暗号化する著作物暗号化手段と、

前記利用条件設定手段で設定された利用条件毎に、異なる複数のチケット暗号鍵及び対応する複数のチケット復号鍵を生成するチケット鍵生成手段と、

前記チケット鍵生成手段が利用条件毎に生成した複数のチケット暗号鍵で、前記所定の暗号鍵に対応する所定の復号鍵をそれぞれ暗号化する復号鍵暗号化手段と、

前記著作物データと、前記復号鍵暗号化手段で暗号化された利用条件毎の前記所定の復号鍵と、前記利用条件とをカプセル化したカプセル化著作物を生成するカプセル化手段と、

前記利用条件設定手段により設定された利用条件と、利用条件毎の暗号化に用いたチケット暗号鍵に対応するチケット復号鍵とを、それぞれ対応付けて蓄積する利用条件蓄積手段と、

外部からの前記著作物データの利用要求に応じて、該利用要求での利用条件に対応付けられて前記利用条件蓄積手段に蓄積されているチケット復号鍵を、前記利用要求の発信元の暗号鍵で暗号化するチケット復号鍵暗号化手段と、

前記チケット復号鍵暗号化手段で暗号化されたチケット復号鍵を、前記利用要求の発信元に配信するチケット配信手段とを備えることを特徴とするデジタル著作物流通システム。

【請求項２】前記カプセル化手段が生成したカプセル化著作物を蓄積するカプセル化著作物蓄積手段と、

前記カプセル化著作物蓄積手段に蓄積されたカプセル化著作物を配信するカプセル化著作物配信手段とをさらに備えることを特徴とする請求項１に記載のデジタル著作物流通システム。

【請求項３】前記所定の暗号鍵と、これに対応する前記復号鍵とは、共通暗号系を用いており、それぞれ同一の鍵であることを特徴とする請求項１または２に記載のデジタル著作物流通システム。

【請求項４】乱数を発生する乱数発生手段をさらに備え、

前記カプセル化著作物の暗号及び復号に使用する共通暗号系の鍵は、前記乱数発生手段が発生した乱数であることを特徴とする請求項３に記載のデジタル著作物流通システム。

【請求項５】前記複数のチケット暗号鍵と、これらのそれぞれに対応するチケット復号鍵とは、共通暗号系を用いており、それぞれ対応するもの同士が同一のチケット鍵で構成され、

前記チケット鍵生成手段は、利用条件毎に暗号と復号とに共通のチケット鍵を生成することを特徴とする請求項

2

１乃至４のいずれか１項に記載のデジタル著作物流通システム。

【請求項６】前記カプセル化手段によってカプセル化されたカプセル化著作物に含まれる著作物データから二次著作物データを生成する二次著作物データ生成手段を備え、前記配布すべき著作物データを、前記二次著作物データ生成手段によって生成された二次著作物データとし、

前記チケット鍵生成手段は、真のチケット暗号鍵及び対応する真のチケット復号鍵を生成する手段と、該真のチケット暗号鍵及び対応する真のチケット復号鍵並びに前記二次著作物データの基となる著作物データのチケット復号鍵から他の他のチケット復号鍵を生成する手段とを備え、

前記復号鍵暗号化手段は、前記二次著作物データの暗号鍵に対応する復号鍵をそれぞれ、前記真のチケット暗号鍵で暗号化し、

前記利用条件蓄積手段は、さらに前記他のチケット復号鍵を対応付けて蓄積することを特徴とする請求項１乃至５のいずれか１項に記載のデジタル著作物流通システム。

【請求項７】前記配布すべき著作物データに対して課金に関する処理を行わせるための課金モジュールを、前記利用条件設定手段によって設定された利用条件毎に生成するする課金モジュール生成手段をさらに備え、

前記利用条件蓄積手段は、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積し、

前記カプセル化手段は、前記課金モジュール生成手段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成することを特徴とする請求項１乃至５のいずれか１項に記載のデジタル著作物流通システム。

【請求項８】前記カプセル化手段がカプセル化したカプセル化著作物を取得するカプセル化著作物取得手段と、

前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得手段と、

前記チケット復号鍵取得手段が取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号手段と、

前記復号鍵復号手段が復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号手段と、

前記著作物復号手段で復号した著作物データを再生する再生手段とをさらに備えることを特徴とする請求項１乃至５のいずれか１項に記載のデジタル著作物流通システム。

【請求項９】前記配布すべき著作物データに対して課金

に関する処理を行わせるための課金モジュールを、前記利用条件設定手段によって設定された利用条件毎に生成するする課金モジュール生成手段をさらに備え、
前記利用条件蓄積手段は、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積し、
前記カプセル化手段は、前記課金モジュール生成手段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成し、
前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる課金モジュールを抽出して蓄積する課金モジュール蓄積手段と、
前記課金モジュール蓄積手段に蓄積されている課金モジュールのうちで、前記チケット鍵取得手段が取得したチケット復号鍵に対応する利用条件に応じたものに従って前記著作物データに対する課金処理を実行する課金処理手段とをさらに備えることを特徴とする請求項８に記載のデジタル著作物流通システム。
【請求項１０】所定の暗号鍵により暗号化された著作物データと、前記著作物データの利用条件と、前記利用条件毎に異なるチケット暗号鍵で暗号化した前記所定の暗号鍵に対応する複数の復号鍵とをカプセル化したカプセル化著作物を取得するカプセル化著作物取得手段と、
前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得手段と、
前記チケット復号鍵取得手段が取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号手段と、
前記復号鍵復号手段が復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号手段と前記著作物復号手段で復号した著作物データを再生する再生手段とを備えることを特徴とするデジタル著作物再生装置。
【請求項１１】前記カプセル化著作物取得手段が取得するカプセル化著作物は、さらに前記著作物データ毎の課金モジュールをカプセル化したものであり、
前記チケット鍵取得手段は、さらに利用条件に応じた課金モジュールに関する情報を取得し、
前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる課金モジュールを抽出して蓄積する課金モジュール蓄積手段と、
前記課金モジュール蓄積手段に蓄積されている課金モジュールのうちで、前記チケット鍵取得手段が取得したチケット復号鍵に対応する利用条件に応じたものに従って前記著作物データに対する課金処理を実行する課金処理手段とをさらに備えることを特徴とする請求項１０に記載のデジタル著作物再生装置。
【請求項１２】配布すべき著作物データに利用条件を設

定する利用条件設定ステップと、
前記著作物データを所定の暗号鍵により暗号化する著作物暗号化ステップと、
前記利用条件設定ステップで設定された利用条件毎に、異なる複数のチケット暗号鍵及び対応する複数のチケット復号鍵を生成するチケット鍵生成ステップと、
前記チケット鍵生成ステップで利用条件毎に生成した複数のチケット暗号鍵で、前記所定の暗号鍵に対応する所定の復号鍵をそれぞれ暗号化する復号鍵暗号化ステップと、
前記著作物データと、前記復号鍵暗号化ステップで暗号化された利用条件毎の前記所定の復号鍵と、前記利用条件とをカプセル化するカプセル化ステップと、前記利用条件設定ステップで設定された利用条件と、利用条件毎の暗号化に用いたチケット暗号鍵に対応するチケット復号鍵とを、それぞれ対応付けて蓄積する利用条件蓄積ステップと、
外部からの前記著作物データの利用要求に応じて、該利用要求での利用条件に対応付けられて蓄積されているチケット復号鍵を、前記利用要求の発信元の暗号鍵で暗号化するチケット復号鍵暗号化ステップと、
前記チケット復号鍵暗号化ステップで暗号化されたチケット復号鍵を、前記利用要求の発信元に配信するチケット配信ステップとを含むことを特徴とするデジタル著作物流通方法。
【請求項１３】前記カプセル化ステップでカプセル化されたカプセル化著作物に含まれる著作物データから二次著作物データを生成する二次著作物データ生成ステップをさらに含み、
前記配布すべき著作物データを、前記二次著作物データ生成手段によって生成された二次著作物データとし、
前記チケット鍵生成ステップは、真のチケット暗号鍵及び対応する真のチケット復号鍵を生成するステップと、該真のチケット暗号鍵及び対応する真のチケット復号鍵並びに前記二次著作物データの基となる著作物データのチケット復号鍵から他の他のチケット復号鍵を生成するステップとを含み、
前記復号鍵暗号化ステップは、前記二次著作物データの暗号鍵に対応する復号鍵をそれぞれ、前記真のチケット暗号鍵で暗号化し、
前記利用条件蓄積ステップは、さらに前記他のチケット復号鍵を対応付けて蓄積することを特徴とする請求項１２に記載のデジタル著作物流通方法。
【請求項１４】前記配布すべき著作物データに対して課金に関する処理を行わせるための課金モジュールを、前記利用条件設定手段によって設定された利用条件毎に生成するする課金モジュール生成ステップをさらに含み、
前記利用条件蓄積ステップは、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積し、
前記カプセル化ステップは、前記課金モジュール生成手

段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成することを特徴とする請求項１２に記載のデジタル著作物流通方法。

【請求項１５】所定の暗号鍵により暗号化された著作物データと、前記著作物の利用条件と、前記利用条件毎に異なるチケット暗号鍵で暗号化した前記所定の暗号鍵に対応する複数の復号鍵とをカプセル化したカプセル化著作物を取得するカプセル化著作物取得ステップと、

取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得ステップと、

前記チケット復号鍵取得ステップで取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号ステップと、

前記復号鍵復号ステップで復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号ステップとを含むことを特徴とするデジタル著作物再生方法。

【請求項１６】配布すべき著作物データに利用条件を設定する利用条件設定ステップと、

前記著作物データを所定の暗号鍵により暗号化する著作物暗号化ステップと、

前記利用条件設定ステップで設定された利用条件毎に、異なる複数のチケット暗号鍵及び対応する複数のチケット復号鍵を生成するチケット鍵生成ステップと、

前記チケット鍵生成ステップで利用条件毎に生成した複数のチケット暗号鍵で、前記所定の暗号鍵に対応する所定の復号鍵をそれぞれ暗号化する復号鍵暗号化ステップと、

前記著作物データと、前記復号鍵暗号化ステップで暗号化された利用条件毎の前記所定の復号鍵と、前記利用条件とをカプセル化するカプセル化ステップと、

前記利用条件設定ステップで設定された利用条件と、利用条件毎の暗号化に用いたチケット暗号鍵に対応するチケット復号鍵とを、それぞれ対応付けて蓄積する利用条件蓄積ステップと、

外部からの前記著作物データの利用要求に応じて、該利用要求での利用条件に対応付けられて蓄積されているチケット復号鍵を、前記利用要求の発信元の暗号鍵で暗号化するチケット復号鍵暗号化ステップと、

前記チケット復号鍵暗号化ステップで暗号化されたチケット復号鍵を、前記利用要求の発信元に配信するチケット配信ステップとを実行するプログラムを記録することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項１７】前記カプセル化ステップでカプセル化されたカプセル化著作物に含まれる著作物データから二次著作物データを生成する二次著作物データ生成ステップをさらに含み、

前記配布すべき著作物データを、前記二次著作物データ生成手段によって生成された二次著作物データとし、

前記チケット鍵生成ステップは、真のチケット暗号鍵及び対応する真のチケット復号鍵を生成するステップと、該真のチケット暗号鍵及び対応する真のチケット復号鍵並びに前記二次著作物データの基となる著作物データのチケット復号鍵から他の他のチケット復号鍵を生成するステップとを含み、

前記復号鍵暗号化ステップは、前記二次著作物データの暗号鍵に対応する復号鍵をそれぞれ、前記真のチケット暗号鍵で暗号化し、

前記利用条件蓄積ステップは、さらに前記他のチケット復号鍵を対応付けて蓄積することを特徴とする請求項１６に記載のコンピュータ読み取り可能な記録媒体。

【請求項１８】前記配布すべき著作物データに対して課金に関する処理を行わせるための課金モジュールを、前記利用条件設定ステップで設定された利用条件毎に生成するする課金モジュール生成ステップをさらに含み、

前記利用条件蓄積ステップは、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積し、

前記カプセル化ステップは、前記課金モジュール生成手段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成することを特徴とする請求項１６に記載のコンピュータ読み取り可能な記録媒体。

【請求項１９】所定の暗号鍵により暗号化された著作物データと、前記著作物の利用条件と、前記利用条件毎に異なるチケット暗号鍵で暗号化した前記所定の暗号鍵に対応する複数の復号鍵とをカプセル化したカプセル化著作物を取得するカプセル化著作物取得ステップと、

取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得ステップと、

前記チケット復号鍵取得ステップで取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号ステップと、

前記復号鍵復号ステップで復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号ステップとを実行するプログラムを記録することを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタル著作物流通システム及び方法、デジタル著作物再生装置及び方法、並びにこれらのプログラムを記録したコンピュータ読み取り可能な記録媒体に関し、特にデジタル著作物の利用制御、二次著作物の利用制御、及びデジタル著作物に対する課金に関する。

【０００２】
【従来の技術】従来、デジタル著作物流通システムは、ソフトウェアやマルチメディアコンテンツを暗号化し、利用者が販売者の示した利用規約に応じて相当額を、クレジットカードや銀行振込や電子現金などを介して、販売者に代金を収めるために用いられている。従来のデジタル著作物流通システムの一例が、特開平９－１３８８２７号公報に記載されている。
【０００３】この公報に記載されたデジタル著作物流通システムは、流通センタ装置と利用者装置から構成されている。流通センタ装置では、利用者装置から要求された著作物について、適当な利用契約を結んだのち、利用者の公開鍵により当該著作物データを暗号化し、利用者装置へ送信する。
【０００４】このとき、著作物データには利用条件が付加されており、前記利用者装置により解釈されて「参照のみ」や「編集可能」などの利用法制御が行なわれる。二次的著作物については、オリジナルデータと二次的著作に相当するデータおよび合成プログラムとがカプセル化され、オリジナルデータと同様に流通センタ装置を介して流通される。課金については、前記利用契約に記載された額の著作物の代金が課金される。
【０００５】その他に、著作物は慣用暗号により暗号化し、所定の代金を支払ったときのみ、当該著作物の復号鍵を配信するような著作物流通システムも一般に良く知られている。一方、１９８８年ＵＳＥＮＩＸカンファレンスプロシーディングス記載のＫｅｒｂｅｒｏｓシステムでは、認証情報Ｉが証明者Ｐが生成したものであることを、慣用暗号を用いて証明する方法が一般によく知られている。
【０００６】この方法によると、１）ＩおよびセッションKp，ｖを含んだ系列を信頼できる第三者が検証者Ｖ固有の鍵により暗号化したもの（チケット）とＫｃ，ｓを証明者Ｐに渡す。２）ＰはチケットをＶに渡すとともに、３）ＩをＫｃ，ｓにより暗号化したもの（認証子）をＶに渡す。４）Ｖは、Ｋｖを使ってチケットよりＩおよびKp，ｖを復号するとともに、Ｋｃ，ｓを使って認証子よりＩを復号し、同じＩが復号されたことを確認する。
【０００７】同様の方法を、前記慣用暗号を利用した流通システムに適用すると、認証情報の代わりに著作物とし、セッション鍵の代わりに利用法に依存して決定される鍵とすると、慣用暗号により暗号化された著作物を配布した上で、利用時にチケット（著作物は含まれない）を配布することで、著作物の利用制御を行うことができる。
【０００８】また、利用者の著作物に対する利用を細かく制限するようなデジタル著作物流通システムでは、著作物に予め利用不可能な利用法を列挙した禁止利用法リストを付加し、著作物視聴装置により、当該リストを解釈して、各種利用法の実行可否を判断する。この種のデジタル著作物流通システムの一例が、特開平９－２６９９１６号公報に記載されている。
【０００９】この公報に記載されたデジタル著作物流通システムは、編集装置と、流通サーバ装置と、視聴装置とを有し、編集装置で著作物データの編集と、禁止利用法リストの作成を行い、両者を一つのカプセル化著作物に同梱する。そして、流通サーバ装置を介して、視聴装置に流通される。視聴装置では、前記カプセル化著作物を開梱し、禁止利用法リストを基に、各利用法に対応するプロセス間メッセージを阻止するようなフックを、視聴装置が動作するオペレーティングシステムに施すことで、前記リストに記載された利用法を禁止する。
【００１０】また、二次的著作物に対する著作権保護を可能とするようなデジタル著作物流通システムでは、二次的著作者が前段の著作物の暗号鍵とは異なる二次暗号鍵を生成し、当該二次暗号鍵により二次的著作物を暗号化して流通させる。このとき、各次暗号鍵は、著作権管理センタにより管理され、以上のような二次的著作が行われたことを把握する。この種のデジタル著作物流通システムの一例が、特開平８－２７２７４５号公報に記載されている。
【００１１】この公報に記載されたデジタル著作物流通システムは、一次著作物が一次暗号鍵により暗号化され、当該一次著作物を利用した二次著作物の作成・配布に際して、二次暗号鍵を新たに生成し、当該二次暗号鍵により前記二次著作物を暗号化し、配布する。当該二次著作物には、前記一次著作物の原データと、当該二次著作物を作成するための加工手順とが、同梱されている。前記一次著作物の原データの復元には、前記一次暗号鍵を用い、前記二次著作物全体を復元には、前記二次暗号鍵を用いる。
【００１２】著作物への課金に関して、利用度数を監視し、利用度数を基にした従量課金を行うことのできる方法が提案されている。このような著作物利用制御システムの一例が、特開平８－９５７７７号公報記載されている。
【００１３】この公報に記載された著作物利用制御システムは、著作物に対して所定の利用が行われたときにその利用度数の計数を行う。当該著作物には、課金情報が含まれており、各利用に関して、一定回数の無料利用ができるような設定の他、利用度数を基にした課金方法を設定できるようになっている。
【００１４】
【発明が解決しようとする課題】しかしながら、上記従来例には、次のような問題点があった。
【００１５】第１の問題点は、著作者や販売者の著作物の配布に関する意図が十分反映されない点にある。その理由は、利用者が受け取ったカプセル化著作物データに対して、ある一つの固定された利用法制御しか行えない

ためである。したがって、異なる利用法制御を行おうとした場合、前記利用条件をいくつか作成し、それぞれについてカプセル化を行う必要があるが、著作者や販売者の意図を反映するに十分とは言えない。

【００１６】第２の問題点は、利用条件を著作物に同梱するのは危険である点にある。その理由は、視聴装置で、利用条件が著作物データと共に不揮発性メモリに保持されるが、この際、利用条件に不正な変更が加えられる可能性があるためである。

【００１７】第３の問題点は、二次的著作物の利用について効率が悪い点にある。その理由は、前記特開平８－２７２７２５号公報に記載されているような方法では、二次的著作物の利用の際、まず当該著作物に含まれる原著作物の復元を行い、さらに当該二次的著作物に追加されたデータを復元する必要がある。通常、画像や動画などの著作物は、そのサイズが膨大であり、前記のような複数回の復号処理を行う方法では、再生処理のスループットの大幅な低下を引き起こすためである。

【００１８】第４の問題点は、流通させる著作物の多様性を保つことが困難な点にある。その理由は、課金方法がシステムにより予め定められていたり、利用度数だけなど課金単位が固定的であったりすると、動画を用いた映画的作品（ペイ・パー・ビュー向き）や書籍的作品（売切向き）など、様々な形態をもった著作物を包括的に扱うことが困難なためである。

【００１９】本発明の第１の目的は、デジタル著作物の流通に関し、著作者および販売者の意図を反映させるために、詳細かつ柔軟な利用条件記述を行う手段を提供することにある。

【００２０】本発明の第２の目的は、デジタル著作物のより強固な安全性を実現することにある。

【００２１】本発明の第３の目的は、二次的著作物の利用において、当該著作物に関係する任意の権原者の権利主張を可能にし、二次的著作物の再生処理時の、暗号化著作物データの復号によるスループット低下を抑制することにある。

【００２２】本発明の第４の目的は、デジタル著作物に対する課金処理の柔軟性向上にある。

【００２３】

【課題を解決するための手段】上記第１、第２の目的を達成するため、本発明の第１の観点にかかるデジタル著作物流通システムは、配布すべき著作物データに利用条件を設定する利用条件設定手段と、前記著作物データを所定の暗号鍵により暗号化する著作物暗号化手段と、前記利用条件設定手段で設定された利用条件毎に、異なる複数のチケット暗号鍵及び対応する複数のチケット復号鍵を生成するチケット鍵生成手段と、前記チケット鍵生成手段が利用条件毎に生成した複数のチケット暗号鍵で、前記所定の暗号鍵に対応する所定の復号鍵をそれぞれ暗号化する復号鍵暗号化手段と、前記著作物データと、前記復号鍵暗号化手段で暗号化された利用条件毎の前記所定の復号鍵と、前記利用条件とをカプセル化したカプセル化著作物を生成するカプセル化手段と、前記利用条件設定手段により設定された利用条件と、利用条件毎の暗号化に用いたチケット暗号鍵に対応するチケット復号鍵とを、それぞれ対応付けて蓄積する利用条件蓄積手段と、外部からの前記著作物データの利用要求に応じて、該利用要求での利用条件に対応付けられて前記利用条件蓄積手段に蓄積されているチケット復号鍵を、前記利用要求の発信元の暗号鍵で暗号化するチケット復号鍵暗号化手段と、前記チケット復号鍵暗号化手段で暗号化されたチケット復号鍵を、前記利用要求の発信元に配信するチケット配信手段とを備えることを特徴とする。

【００２４】上記デジタル著作物流通システムでは、配信されるカプセル化著作物にはその著作物データの復号鍵が含まれていないため、著作物データを自由に配布することが可能となる。そして、著作物データを利用させる場合には、チケット配信手段からチケット復号鍵を配信するだけでよく、著作物の流通範囲の拡大と利用促進を望めるようになる。

【００２５】また、利用条件設定手段によって著作物データの利用条件が設定され、その利用条件毎に異なるチケット鍵（暗号鍵及び復号鍵）が生成される。このため、著作者及び販売者の意図を反映させて、利用条件を設定し、著作物データを利用させることができる。

【００２６】上記デジタル著作物流通システムは、前記カプセル化手段が生成したカプセル化著作物を蓄積するカプセル化著作物蓄積手段と、前記カプセル化著作物蓄積手段に蓄積されたカプセル化著作物を配信するカプセル化著作物配信手段とをさらに備えるものとしてもよい。

【００２７】上記デジタル著作物流通システムにおいて、前記所定の暗号鍵と、これに対応する前記復号鍵とは、共通暗号系を用いて、それぞれ同一の鍵とすることができる。

【００２８】上記デジタル著作物流通システムは、乱数を発生する乱数発生手段をさらに備えるものとすることができる。この場合、前記カプセル化著作物の暗号及び復号に使用する共通暗号系の鍵は、前記乱数発生手段が発生した乱数とすることができる。

【００２９】また、上記デジタル著作物流通システムにおいて、前記複数のチケット暗号鍵と、これらのそれぞれに対応するチケット復号鍵とは、共通暗号系を用いて、それぞれ対応するもの同士が同一のチケット鍵で構成されたものとすることができる。この場合、前記チケット鍵生成手段は、利用条件毎に暗号と復号とに共通のチケット鍵を生成するものとすることができる。

【００３０】さらに上記第３の目的を達成するため、上記デジタル著作物流通システムは、前記カプセル化手段によってカプセル化されたカプセル化著作物に含まれる

著作物データから二次著作物データを生成する二次著作物データ生成手段を備えるものとしてもよい。この場合、前記配布すべき著作物データを、前記二次著作物データ生成手段によって生成された二次著作物データとすることができる。そして、前記チケット鍵生成手段は、真のチケット暗号鍵及び対応する真のチケット復号鍵を生成する手段と、該真のチケット暗号鍵及び対応する真のチケット復号鍵並びに前記二次著作物データの基となる著作物データのチケット復号鍵から他の他のチケット復号鍵を生成する手段とを備え、前記復号鍵暗号化手段は、前記二次著作物データの暗号鍵に対応する復号鍵をそれぞれ、前記真のチケット暗号鍵で暗号化し、前記利用条件蓄積手段は、さらに前記他のチケット復号鍵を対応付けて蓄積するものとすることができる。

【００３１】この場合、二次著作物データを一次著作物データと同様に流通させることができるので、著作活動の活性化が可能となる。また、二次著作物データの利用には真のチケット復号鍵が必要となるが、このためには、その基となる著作物データのチケット復号鍵と前記他のチケット復号鍵とが必要となるので、一次著作者の権利保護を十分に図ることができる。

【００３２】さらに上記第４の目的を達成するため、上記デジタル著作物流通システムは、前記配布すべき著作物データに対して課金に関する処理を行わせるための課金モジュールを、前記利用条件設定手段によって設定された利用条件毎に生成するする課金モジュール生成手段をさらに備えるものとすることができる。この場合、前記利用条件蓄積手段は、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積し、前記カプセル化手段は、前記課金モジュール生成手段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成することができる。

【００３３】この場合、課金処理が課金モジュールで行われることとなり、しかも利用条件毎に生成が可能であるため、著作者や販売者の意図、或いは著作物の性格などに従って、適切な課金方法を柔軟に選択することができる。

【００３４】また、上記デジタル著作物流通システムは、前記カプセル化手段がカプセル化したカプセル化著作物を取得するカプセル化著作物取得手段と、前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得手段と、前記チケット復号鍵取得手段が取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号手段と、前記復号鍵復号手段が復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号手段と、前記著作物復号手段で復号した著作物データを再生する再生手段とをさらに備えるものとすることができる。

【００３５】このような構成とした場合には、上記デジタル著作物流通システムは、前記配布すべき著作物データに対して課金に関する処理を行わせるための課金モジュールを、前記利用条件設定手段によって設定された利用条件毎に生成するする課金モジュール生成手段をさらに備えるものとし、前記利用条件蓄積手段は、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積するものとすることができる。この場合、前記カプセル化手段は、前記課金モジュール生成手段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成するものとなる。そして、上記デジタル著作物流通システムは、前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる課金モジュールを抽出して蓄積する課金モジュール蓄積手段と、前記課金モジュール蓄積手段に蓄積されている課金モジュールのうちで、前記チケット鍵取得手段が取得したチケット復号鍵に対応する利用条件に応じたものに従って前記著作物データに対する課金処理を実行する課金処理手段とをさらに備えるものとすることができる。

【００３６】上記第１、第２の目的を達成するため、本発明の第２の観点にかかるデジタル著作物再生装置は、所定の暗号鍵により暗号化された著作物データと、前記著作物データの利用条件と、前記利用条件毎に異なるチケット暗号鍵で暗号化した前記所定の暗号鍵に対応する複数の復号鍵とをカプセル化したカプセル化著作物を取得するカプセル化著作物取得手段と、前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得手段と、前記チケット復号鍵取得手段が取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号手段と、前記復号鍵復号手段が復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号手段と前記著作物復号手段で復号した著作物データを再生する再生手段とを備えることを特徴とする。

【００３７】さらに上記第４の目的を達成するため、上記デジタル著作物再生装置において、前記カプセル化著作物取得手段が取得するカプセル化著作物は、さらに前記著作物データ毎の課金モジュールをカプセル化したものとし、前記チケット鍵取得手段は、さらに利用条件に応じた課金モジュールに関する情報を取得するものとすることができる。この場合、上記デジタル著作物再生装置は、前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる課金モジュールを抽出して蓄積する課金モジュール蓄積手段と、前記課金モジュール蓄積手段に蓄積されている課金モジュールのうちで、前

記チケット鍵取得手段が取得したチケット復号鍵に対応する利用条件に応じたものに従って前記著作物データに対する課金処理を実行する課金処理手段とをさらに備えるものとすることができる。

【００３８】上記第１、第２の目的を達成するため、本発明の第３の観点にかかるデジタル著作物流通方法は、配布すべき著作物データに利用条件を設定する利用条件設定ステップと、前記著作物データを所定の暗号鍵により暗号化する著作物暗号化ステップと、前記利用条件設定ステップで設定された利用条件毎に、異なる複数のチケット暗号鍵及び対応する複数のチケット復号鍵を生成するチケット鍵生成ステップと、前記チケット鍵生成ステップで利用条件毎に生成した複数のチケット暗号鍵で、前記所定の暗号鍵に対応する所定の復号鍵をそれぞれ暗号化する復号鍵暗号化ステップと、前記著作物データと、前記復号鍵暗号化ステップで暗号化された利用条件毎の前記所定の復号鍵と、前記利用条件とをカプセル化するカプセル化ステップと、前記利用条件設定ステップで設定された利用条件と、利用条件毎の暗号化に用いたチケット暗号鍵に対応するチケット復号鍵とを、それぞれ対応付けて蓄積する利用条件蓄積ステップと、外部からの前記著作物データの利用要求に応じて、該利用要求での利用条件に対応付けられて蓄積されているチケット復号鍵を、前記利用要求の発信元の暗号鍵で暗号化するチケット復号鍵暗号化ステップと、前記チケット復号鍵暗号化ステップで暗号化されたチケット復号鍵を、前記利用要求の発信元に配信するチケット配信ステップとを含むことを特徴とする。

【００３９】さらに上記第３の目的を達成するため、上記デジタル著作物流通方法は、前記カプセル化ステップでカプセル化されたカプセル化著作物に含まれる著作物データから二次著作物データを生成する二次著作物データ生成ステップをさらに含むものとすることができる。この場合、前記配布すべき著作物データを、前記二次著作物データ生成手段によって生成された二次著作物データとしてもよい。そして、前記チケット鍵生成ステップは、真のチケット暗号鍵及び対応する真のチケット復号鍵を生成するステップと、該真のチケット暗号鍵及び対応する真のチケット復号鍵並びに前記二次著作物データの基となる著作物データのチケット復号鍵から他の他のチケット復号鍵を生成するステップとを含み、前記復号鍵暗号化ステップは、前記二次著作物データの暗号鍵に対応する復号鍵をそれぞれ、前記真のチケット暗号鍵で暗号化し、前記利用条件蓄積ステップは、さらに前記他のチケット復号鍵を対応付けて蓄積するものとすることができる。

【００４０】さらに上記第４の目的を達成するため、上記デジタル著作物流通方法は、前記配布すべき著作物データに対して課金に関する処理を行わせるための課金モジュールを、前記利用条件設定手段によって設定された利用条件毎に生成するする課金モジュール生成ステップをさらに含むものとしてもよい。この場合、前記利用条件蓄積ステップは、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積し、前記カプセル化ステップは、前記課金モジュール生成手段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成するものとすることができる。

【００４１】上記第１、第２の目的と達成するため、本発明の第４の観点にかかるデジタル著作物再生方法は、所定の暗号鍵により暗号化された著作物データと、前記著作物の利用条件と、前記利用条件毎に異なるチケット暗号鍵で暗号化した前記所定の暗号鍵に対応する複数の復号鍵とをカプセル化したカプセル化著作物を取得するカプセル化著作物取得ステップと、取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得ステップと、前記チケット復号鍵取得ステップで取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号ステップと、前記復号鍵復号ステップで復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号ステップとを含むことを特徴とする。

【００４２】上記第１、第２の目的を達成するため、本発明の第５の観点にかかるコンピュータ読み取り可能な記録媒体は、配布すべき著作物データに利用条件を設定する利用条件設定ステップと、前記著作物データを所定の暗号鍵により暗号化する著作物暗号化ステップと、前記利用条件設定ステップで設定された利用条件毎に、異なる複数のチケット暗号鍵及び対応する複数のチケット復号鍵を生成するチケット鍵生成ステップと、前記チケット鍵生成ステップで利用条件毎に生成した複数のチケット暗号鍵で、前記所定の暗号鍵に対応する所定の復号鍵をそれぞれ暗号化する復号鍵暗号化ステップと、前記著作物データと、前記復号鍵暗号化ステップで暗号化された利用条件毎の前記所定の復号鍵と、前記利用条件とをカプセル化するカプセル化ステップと、前記利用条件設定ステップで設定された利用条件と、利用条件毎の暗号化に用いたチケット暗号鍵に対応するチケット復号鍵とを、それぞれ対応付けて蓄積する利用条件蓄積ステップと、外部からの前記著作物データの利用要求に応じて、該利用要求での利用条件に対応付けられて蓄積されているチケット復号鍵を、前記利用要求の発信元の暗号鍵で暗号化するチケット復号鍵暗号化ステップと、前記チケット復号鍵暗号化ステップで暗号化されたチケット復号鍵を、前記利用要求の発信元に配信するチケット配信ステップとを実行するプログラムを記録することを特徴とする。

【００４３】さらに上記第３の目的を達成するため、上記記録媒体は、前記カプセル化ステップでカプセル化さ

れたカプセル化著作物に含まれる著作物データから二次著作物データを生成する二次著作物データ生成ステップを実行するプログラムをさらに記録するものとすることができる。この場合、前記配布すべき著作物データを、前記二次著作物データ生成手段によって生成された二次著作物データとしてもよい。そして、前記チケット鍵生成ステップは、真のチケット暗号鍵及び対応する真のチケット復号鍵を生成するステップと、該真のチケット暗号鍵及び対応する真のチケット復号鍵並びに前記二次著作物データの基となる著作物データのチケット復号鍵から他の他のチケット復号鍵を生成するステップとを含み、前記復号鍵暗号化ステップは、前記二次著作物データの暗号鍵に対応する復号鍵をそれぞれ、前記真のチケット暗号鍵で暗号化し、前記利用条件蓄積ステップは、さらに前記他のチケット復号鍵を対応付けて蓄積するものとすることができる。

【００４４】さらに上記第４の目的を達成するため、上記記録媒体は、前記配布すべき著作物データに対して課金に関する処理を行わせるための課金モジュールを、前記利用条件設定手段によって設定された利用条件毎に生成するする課金モジュール生成ステップを実行するプログラムをさらに記録するものとしてもよい。この場合、前記利用条件蓄積ステップは、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積し、前記カプセル化ステップは、前記課金モジュール生成手段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成するものとすることができる。

【００４５】上記第１、第２の目的と達成するため、本発明の第の６観点にかかる記録媒体は、所定の暗号鍵により暗号化された著作物データと、前記著作物の利用条件と、前記利用条件毎に異なるチケット暗号鍵で暗号化した前記所定の暗号鍵に対応する複数の復号鍵とをカプセル化したカプセル化著作物を取得するカプセル化著作物取得ステップと、取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得ステップと、前記チケット復号鍵取得ステップで取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号ステップと、前記復号鍵復号ステップで復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号ステップとを実行するプログラムを記録することを特徴とする。

【００４６】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。

【００４７】［第１の実施の形態］図１を参照すると、本発明の第１の実施の形態の著作物流通システムは、著作物データとその利用条件を編集し、カプセル化し、暗号化する編集装置１と、チケットと利用条件を管理するチケットサーバ装置２と、暗号化された著作物を配布する流通センタ装置３と、利用者が著作物を利用する視聴装置４を含む。編集装置１は、著作者が保有し、チケットサーバ装置２および流通センタ装置３は、著作者もしくは販売代行者が保有・管理する。視聴装置４は、利用者が保有する。

【００４８】編集装置１は、キーボード／マウスなどのユーザ入力部１１と、モニタなどのユーザ出力部１２と、利用条件設定部１３と、編集処理部１４と、カプセル化処理部１５と、登録インターフェース部１６を備えている。

【００４９】利用条件設定部１３は、編集処理部１４で作成された著作物データに対する利用条件を、ユーザ入力部１１とユーザ出力部１２を介して著作者と対話的に作成する。

【００５０】編集処理部１４は、ユーザ入力部１１からの入力に応じて著作物データを作成し、同時に作成された著作物データをユーザ出力部１２に表示する。カプセル化処理部１５は、暗号化手段１５１と、チケット鍵生成手段１５２と、乱数発生手段１５３とを備えており、乱数発生手段１５３より得られた一つの乱数Ｒと、チケット鍵生成手段１５２から得られた各チケット鍵を、暗号化手段１５１を用いて暗号化し、その結果から利用情報テーブルを作成するとともに、前記乱数Ｒと編集処理部１４で作成された著作物データとを、暗号化手段１５１を用いて暗号化し、その結果と前記利用情報テーブルとを結合したカプセル化著作物データを生成する。

【００５１】登録インターフェース部１６は、チケットサーバ装置２へ前段までで生成した利用条件とチケット鍵を登録するための通信を行う。また、登録インターフェース部１６は、流通センタ装置３へカプセル化著作物を蓄積するための通信を行う。

【００５２】チケットサーバ装置２は、登録インターフェース部２１と、利用条件蓄積部２２と、利用条件判定部２３と、チケット生成部２４と、チケット暗号化部２５と、配信インターフェース部２６を備えている。

【００５３】登録インターフェース部２１は、編集装置１により作成された利用条件とチケット鍵の登録に伴う通信を行う。

【００５４】利用条件蓄積部２２は、登録インターフェース部２１より得た利用条件およびチケット鍵を蓄積する。

【００５５】利用条件判定部２３は、配信インターフェース部２６より得られた要求が利用条件に合致するかどうかを判定する。

【００５６】チケット生成部２４は、利用条件蓄積部２２より利用条件とチケット鍵とから、チケットを生成する。

【００５７】チケット暗号化部２５は、利用条件判定部

２３で合致すると判定された場合に適切なチケットを利用条件蓄積部２２より取り出して利用者に応じて暗号化する。

【００５８】配信インターフェース部２６は、視聴装置４からの要求を受信するための通信を行い、チケット暗号化部２５により生成された暗号化チケットを視聴装置４に送信するための通信を行う。

【００５９】流通センタ装置３は、登録インターフェース部３１と、カプセル化著作物蓄積部３２と、配信インターフェース部３３を備える。

【００６０】登録インターフェース部３１は、編集装置２で生成されたカプセル化著作物を受信するための通信を行なう。

【００６１】カプセル化著作物蓄積部３２は、登録インターフェース部３１より受信されたカプセル化著作物を蓄積する。

【００６２】配信インターフェース部３３は、カプセル化著作物蓄積部３２に蓄積された著作物のリストを作成し、視聴装置４へ送信するための通信と、視聴装置４からの要求を受信し、当該要求に応じたカプセル化著作物をカプセル化著作物蓄積部３２より取り出し、視聴装置４へ送信するための通信とを行なう。

【００６３】視聴装置４は、キーボード／マウスなどのユーザ入力部４１と、モニタなどのユーザ出力部４２と、再生処理部４３と、チケットインターフェース部４４と、チケット蓄積部４５と、カプセル化著作物インターフェース部４６と、カプセル化著作物蓄積部４７と、カプセル化解除部４８と、を備える。

【００６４】再生処理部４３は、カプセル化解除部４８より得られた著作物データに記述されたプログラムを実行しながら、その入出力をユーザ入力部４１とユーザ出力部４２を介して行う。

【００６５】チケットインターフェース部４４は、再生処理部４３を介してユーザから要求されたカプセル化著作物およびその利用法に応じて、チケットサーバ装置１よりチケットを受信するための通信を行う。

【００６６】チケット蓄積部４５は、チケットインターフェース部４４より得たチケットを蓄積する。

【００６７】カプセル化著作物インターフェース部４６は、流通センタ装置３から著作物のリストを受信するための通信と、そのリストをユーザ出力部４２に表示し、ユーザ入力部４１により所望の著作物をユーザに選択してもらい、その結果に応じて流通センタ装置３から当該著作物を受信するための通信とを行う。

【００６８】カプセル化著作物蓄積部４７は、カプセル化著作物インターフェース部４３より得られたカプセル化著作物を蓄積する。

【００６９】カプセル化解除部４８は、復号手段４８１を備えており、再生処理部４３を介してユーザから要求されたカプセル化著作物を、カプセル化著作物蓄積部４７より取得し、チケット蓄積部４５より当該カプセル化著作物のチケットを取得し、当該カプセル化著作物および当該チケットから、復号手段４８１を用いて、著作物データを復元する。

【００７０】なお、図１の著作物流通システムにおいて、編集装置１とチケットサーバ装置２、編集装置１と流通センタ装置３、チケットサーバ装置２と視聴装置４、流通センタ装置３と視聴装置４は、それぞれ互いにインターネットなどのネットワークを介して接続される。

【００７１】以下、本実施の形態の動作について説明する。

【００７２】まず、本実施の形態の動作全体の流れについて、図２を参照して説明する。著作者は、編集装置１を用いて著作物データの編集して流通センタ装置３に登録し、また、編集装置１を用いて利用条件の設定してチケットサーバ装置２に登録する（ステップＡ）。

【００７３】次に、利用者は、流通センタ装置３から所望の著作物を取得し、視聴装置４に蓄積する（ステップＢ）。さらに、利用者は、その著作物について利用要求を行い、当該著作物のチケットをチケットサーバ装置２から取得して視聴装置４に蓄積する（ステップＣ）。そして、その利用者は、視聴装置４で当該著作物を利用する（ステップＤ）。

【００７４】次に、図２のステップＡの処理について、図３を参照して詳細に説明する。編集装置１で、著作者は著作物データを作成する。編集処理部１４は一般的なマルチメディアオーサリングソフトウェアと同等の機能を備えており、対話的に著作物を作成することができる（ステップＡ１）。

【００７５】そして当該著作物を流通させようとした時に、著作者は当該著作物に対する利用条件を設定する。この操作は、利用条件設定部１３で制御され、図６のようなダイアログをユーザ出力部１２を介して表示し、著作者はユーザ入力部１１を操作して、図７のような手順で、利用法ごとの条件を設定していく（ステップＡ２）。

【００７６】次に、カプセル化処理部１５で、前段までで作成された著作物データと利用条件とからカプセル化著作物を生成する。

【００７７】まず、暗号化手段１５１で、前記著作物データを乱数発生手段１５３より得た乱数Ｒにより暗号化する（ステップＡ３）。この際、共通鍵暗号を用いれば、暗号化および復号の処理にかかる時間を短くできる。

【００７８】また、利用条件が設定された利用法ｕごとに、乱数発生手段１５３より乱数Ｒｕを得ながら、チケット鍵生成部１５２によりＲｕを鍵として、前記著作物データ暗号鍵Ｒを暗号化手段１５１を用いて暗号化し、利用秘密情報Ｅ［Ｒｕ］（Ｒ）を得ていく（ステップＡ

４）。当該手順を示した模式図を図８に示す。ここで、式Ｅ［Ｋ］（Ｄ）はデータＤを鍵Ｋで共通鍵暗号化した結果を表し、以下同様の表記を用いる。

【００７９】そして、前記利用条件と前記利用秘密情報から、図９に示すような利用法と利用秘密情報の組から成る表を作成する。これを利用秘密情報テーブルと呼ぶ。そして、前記利用秘密情報テーブルと前記暗号化著作物データと、著作者の氏名などで代表される著作者ＩＤや著作物の名称である著作物ＩＤやチケット発行元などの著作物情報とを連結して、図１０に示したような構造をもつカプセル化著作物を生成する（ステップＡ５）。

【００８０】前記利用条件は、図１１に示すようなアクセス制御言語による形式的記述に変換される（ステップＡ６）。アクセス制御言語は、著作物を構成するオブジェクトごとに、可能な利用法が宣言され、利用法ごとに利用条件が宣言される形になっており、前記チケット鍵Ｒｕは、利用法ｕに対する宣言中に埋め込まれる。すなわちオブジェクトを特定するＩＤを示し、次に利用法を表す文字列が示され、各種利用条件を表した条件語と各条件語へのパラメータを列挙し、次にチケット鍵を示す。ここでオブジェクトは、画像／テキストなどの基本的な構成要素を指す。

【００８１】この場合、「モノクロ表示による閲覧」や「フルカラー表示による閲覧」などといったように、利用法をより詳細化して設定する場合には、例えば「モノクロ表示用オブジェクト」や「フルカラー表示用オブジェクト」などを用意し、視聴装置４で、特定機能を利用する場合に、それに応じたオブジェクトに対してチケットの発行を要求すればよい。また、特定機能とその対象となるオブジェクトの関係は、編集装置１４での編集作業時に指定し、カプセル化著作物に当該情報を同梱すればよい。

【００８２】基本的な構成要素の組み合わせや著作物全体といったように、オブジェクトに木構造を設ける場合について、利用条件を付す場合、上位のオブジェクトに属する下位のオブジェクト全てに共通した利用条件として宣言することもできる。まず、上位のオブジェクトを特定するＩＤを示し、次にその直接の子にあたるオブジェクトを示すＩＤを列挙し、次に前記同様、利用法を表す文字列が示され、条件語とそのパラメータの組を列挙する。ただし、最下位オブジェクトにおけるチケット鍵の宣言は、上位オブジェクトに対しては不用である。

【００８３】例を示すと、構成要素１～７をもつ著作物があって、その構成要素間の構造が図１２（ａ）に示した形になっているとする。このとき、利用条件記述は、例えば図１２（ｂ）のようになる。

【００８４】このような形の利用条件記述がチケットサーバ装置２で解釈される際には、各オブジェクトの利用条件は、先祖にあたるオブジェクトで宣言された利用条件を継承する。ただし、上位のオブジェクトにおいてある条件が示され、同条件が、その子孫にあたるオブジェクトでも示されているとき、子孫にあたるオブジェクトの条件が優先される。

【００８５】例えば、前記の例を用いると、（１）著作物全体に対して「表示可能な解像度が６４０×４８０以下」、（２）構成要素３に対して「構成要素１個当りの代金が１０円」、（３）構成要素６に対して「代金が５０円」とあった場合、構成要素６の代金は５０円であり、表示可能解像度は６４０×４８０以下となる。一方、（４）構成要素７に対して「表示可能解像度が８００×６００以下」とあった場合、（１）および（２）および（４）より、構成要素７の代金は１０円であり、表示可能解像度は８００×６００以下となる。

【００８６】以上のようにして生成された利用条件記述は、登録インターフェース部１６を通して、チケットサーバ装置２に登録される（ステップＡ７）。

【００８７】そして、前記カプセル化著作物は、登録インターフェース部１６を通して、流通センタ装置３に登録される（ステップＡ８）。

【００８８】次に、図２のステップＢの処理について、図４を参照して詳細に説明する。視聴装置４で、利用者はまず流通センタ装置３にアクセスし、著作物のカタログを得る（ステップＢ１）。このとき、例えば図１３のようなインデックス画面がユーザ出力４２を介して表示される。

【００８９】利用者は、当該インデックス画面に表示された任意のリンクを辿り、希望の著作物を選択する（ステップＢ２）。当該要求を受けた流通センタ装置３では、カプセル化著作物蓄積部３２より当該要求に応じて適切なカプセル化著作物を取得し、配信インターフェース部３３を介して送信する。

【００９０】視聴装置４では、当該カプセル化著作物を、カプセル化著作物インターフェース部４６を介して受け取ったのち、カプセル化著作物蓄積部４７に蓄積する（ステップＢ３）。

【００９１】次に、図２のステップＣの処理について、図５を参照して詳細に説明する。まず、利用者は、ステップＢ３でカプセルか著作物蓄積部４７に蓄積した当該カプセル化著作物について、任意の利用法により利用要求を行う（ステップＣ１）。

【００９２】前段で蓄積されたカプセル化著作物について、再生処理部４３は利用法ｕについての処理を行なうため、まずカプセル化解除部４８によって、当該カプセル化著作物に含まれる前記著作物情報と、前記利用秘密情報テーブルと、前記暗号化著作物データとに分割する。この分割後、カプセル化解除部４８は、まず必要なチケットを既に取得済みかどうかを調べ、取得済みであれば、当該チケットを用いて後段の暗号化著作物データの復号を行なう。一方、未取得であった場合は、前記著

作物情報中のチケット発行元を参照して、対象となるチケットサーバ装置２を定め、チケットインターフェース部４４を介して、当該チケットサーバ装置２に利用法ｕに対するチケットを要求する（ステップＣ２）。

【００９３】チケットの要求には、「著作者ＩＤ」、「著作物ＩＤ」、「要求元利用者ＩＤ」、「要求する利用法」などの、利用対象である著作物と利用法を特定する情報と、「要求年月日」などの後に当該チケットの取引を証明するに十分な情報と、視聴装置４のユーザ表示部４２の解像度や色数の上限などの表示性能およびユーザからの指示などから決定される利用時の条件が含まれる。

【００９４】当該要求を受けたチケットサーバ装置２は、利用条件蓄積部２２に蓄積された中から当該要求の対象となる著作物の利用条件を参照する（ステップＣ３）。

【００９５】そして、当該利用条件を利用条件判定部２３により解釈し、当該要求に対して前記利用法ｕのチケットを発行してよいかどうかを判定する（ステップＣ４）。判定項目としては、例えば「チケットを発行してよい利用者ＩＤのリスト」があり、この場合前記要求に記載された利用者ＩＤが前記リストに含まれれば当該チケットの発行を許可し、そうでなければ許可しない。不許可と判定された場合は、その旨を視聴装置４に通知し（ステップＣ５’）、視聴装置４では当該チケットの発行が不許可になった旨をユーザ出力部４２を介してユーザに知らせる（ステップＣ６’）。この際、利用法ｕによる利用を行うことはできない。

【００９６】前段で、発行してよいと判定された場合、チケット生成部２４では、前記利用条件の前記利用法についての条件が記述されたブロックを参照し、適切なチケット鍵を取得する。当該チケット鍵と、要求に記載された「利用者ＩＤ」、「利用法」などの前記要求に合致することを証明するに十分な情報を連結して、前記要求に対するチケットを生成する（ステップＣ５）。例えば、図１４に示すように、「著作物ＩＤ」・「利用者ＩＤ」・「チケットシリアル番号」・「チケット鍵」・「許可された利用法」・「発行年月日」・「有効期限」を記載する。

【００９７】当該チケットは、チケット暗号化部２５により、前記利用者側の視聴装置４でのみ復号できるように、暗号化され、配信インターフェース部２６により、前記視聴装置４に送信される（ステップＣ６）。この際、公開鍵暗号を用いることが望ましいが、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵共有プロトコルなどを用いて要求ごとに異なるセッション鍵を生成し、共通鍵暗号により暗号化してもよい。

【００９８】視聴装置４では、当該チケットをチケットインターフェース部４４により受信し、利用者の秘密鍵や前記セッション鍵などを用いて復号化し、チケット蓄積部４５に蓄積する（ステップＣ７）。

【００９９】カプセル化解除部４８は、前記利用法ｕに対するチケットと、前記アクセス制御テーブル中の閲覧ブロックを参照して（ステップＣ８）、それぞれから前記チケット鍵Ｒｕと前記利用秘密情報Ｅ［Ｒｕ］（Ｒ）を取り出し（ステップＣ９）、復号手段４８１を用いて、前記著作物復号鍵Ｒを復元する（ステップＣ１０）。

【０１００】そして、当該復号鍵Ｒと前記暗号化著作物データから、再び復号手段４８１を用いて著作物データを復元する。（ステップＣ１１）。

【０１０１】次に、図２のステップＤの処理について、詳細に説明する。再生処理部４３は一時的な揮発性メモリを備えており、前段で復元された著作物データを当該揮発性メモリに保持する。そして、著作物データの内容を実行し、ユーザ入力部４１とユーザ出力部４２とを介して利用者と著作物との対話を処理する。

【０１０２】以上説明したように、本実施の形態では、著作物が暗号化され、上記利用秘密情報と共にカプセル化され、インターネットなどのネットワーク上で流通される。利用秘密情報は、暗号化された著作物データの復号鍵そのものではなく、復号鍵を得るには別途上記チケットを入手する必要がある。したがって、カプセル化された著作物は複製自由であり、上記流通センタ装置３を必ずしも経ずに、利用者間で譲渡しあうことができるため、著作物の流通速度の向上と、流通範囲の拡大につながる。また、利用法ごとにチケットが発行されるため、チケット１枚あたりの価格を低く抑えることができ、著作物の利用推進につながる。

【０１０３】［第２の実施の形態］図１５を参照すると、本発明の第２の実施の形態の著作物流通システムは、図１に示された第１の実施の形態のものに加え、第１の視聴装置５を有する点で異なる。そして、編集装置７について、第１の実施の形態における編集装置１のカプセル化処理部１５の構成に加え、鍵分割手段６５４を有する点で異なる。また、第２の視聴装置７について、第１の実施の形態における視聴装置４のカプセル化解除部の構成に加え、鍵統合手段７８２を有する点で異なる。

【０１０４】第１の視聴装置５は、図１に示された第１の実施の形態における視聴装置４と同様の構成であるが、ユーザ入力部４１の指示により、カプセル化解除部４８で復元された著作物データを編集装置６の編集処理部１４に受け渡すことができる点で異なる。

【０１０５】鍵分割手段６５４は、カプセル化処理部１５で、第１の視聴装置４により入手した第１のカプセル化著作物に対し、編集処理部１４により再編集を加えた著作物データについて、第２のカプセル化著作物を作成する際に、第１のカプセル化著作物に対する第１のチケット鍵と乱数発生手段１５３から得た真のチケット鍵と

から、第２のカプセル化著作物に対する第２のチケット鍵を生成する。

【０１０６】鍵統合手段７８２は、第２のカプセル化著作物を利用するために、第１のチケット鍵および第２のチケット鍵とから、真のチケット鍵を復元する。

【０１０７】なお、図２の著作物流通システムでは、第１の視聴装置５と編集装置６とが、インターネットなどのネットワークを介して接続される。また、第１の視聴装置５及び第２の視聴装置７は、いずれもインターネットなどのネットワークを介してチケットサーバ装置２及び流通センタ装置３とそれぞれ接続される。

【０１０８】以下、本実施の形態の動作について、説明する。

【０１０９】まず、本実施の形態の動作全体の概略について、図１６を参照して説明する。一次著作者は、第１の実施の形態と同様にして、第１のカプセル化著作物を作成する（ステップＡ）。

【０１１０】二次著作者は、第１の視聴装置５で、第１の実施の形態で利用者がしたのと同様に、前記第１の著作物を取得する（ステップＢ）。そして、二次著作者は、再編集を要求し、その再編集要求を受けた第１の視聴装置５は、第１の実施の形態における視聴装置４と同様にチケットサーバ装置２に対して再編集チケットを要求する。そして、当該チケット要求を受けたチケットサーバ装置２では、再編集に対する利用条件判定を行い、当該条件が満たされれば、再編集チケットを第１の視聴装置５に送信する、これにより二次著作者は、再編集チケットを取得する（ステップＣ）。さらに、編集装置６を用いて著作物データの編集して流通センタ装置３に登録し、また、編集装置６を用いて利用条件の設定してチケットサーバ装置２に登録する（ステップＡ１）。

【０１１１】次に、利用者は、第２の視聴装置７で、前記第２のカプセル化著作物を取得する（ステップＢ２）。さらに、利用者は、その第２のカプセルか著作物著作物について利用要求を行い、当該著作物のチケットをチケットサーバ装置２から取得して視聴装置４に蓄積する（ステップＣ）。そして、再生処理部４３では当該著作物データを本発明の第１の実施の形態と同様の方法で再生する（ステップＤ）。

【０１１２】次に、図１６のステップＡ’の処理について、図１７を参照して詳細に説明する。当該再編集チケットを受信した第１の視聴装置５は、第１の実施の形態における視聴装置４と同様にして、再編集チケットを用いて第１の著作物データを復元し、編集装置６に渡す。その後、編集装置５における編集処理部１４により、二次著作者は当該著作物データを再編集し、第２の著作物データを作成する（ステップＡ’１）。

【０１１３】二次著作者は、第２の著作物データに対して、利用条件設定部１３で、第１の実施の形態における利用条件設定と同様の操作を行った後（ステップＡ’２）、編集装置５は、暗号化手段１５１と乱数発生手段１５３を用いて、第２の著作物データを暗号化する（ステップＡ’３）。

【０１１４】その後、編集装置５は、条件が設定された各利用法Ｕについて、前記第１のカプセル化著作物に対して、利用法Ｕの第１のチケットＴ１をチケットサーバ装置２より入手し、次のようにして、利用法Ｕの第２のチケットＴ２を得る。

【０１１５】チケット鍵生成手段１５２により、前記第２のチケットＴ２を生成する際、まず乱数発生手段１５３で、乱数Ｒを得る（ステップＡ’４－１）。以下、当該乱数Ｒを、真のチケット鍵と呼ぶ。

【０１１６】そして、鍵分割手段６５４で、前記真のチケット鍵Ｒと、第１のチケットＴ１のチケット鍵Ｋ１を用いて、数式１により第２のチケットＴ２のチケット鍵Ｋ２を算出する（ステップＡ’４－２）。なお、当該手順を示した模式図を図１９に示す。

【０１１７】

【数１】Ｋ２　＝　ｆ（Ｋ１，　Ｒ）

【０１１８】ここで、関数ｆは、次の数式２と数式３とを同時に満たす。

【０１１９】

【数２】｜ｆ（ａ，ｂ）｜～｜ａ｜～｜ｂ｜

（｜ｘ｜は正整数ｘのビット数を示し、～は近似であることを示す）

【数３】ｆ（ｂ１，ｂ２）　＝　ｆ（ｂ２，ｂ１）

【０１２０】また、関数ｆは、ａ＝ｆ（ｂ１，ｂ２）のとき、次の数式４及び数式５となる逆関数ｆｉｎｖが存在するような、関数である。

【数４】ｂ２　＝　ｆｉｎｖ（ｂ１，ａ）　＝　ｆｉｎｖ（ａ，ｂ１）

【数５】ｂ１　＝　ｆｉｎｖ（ａ，ｂ２）　＝　ｆｉｎｖ（ｂ２，ａ）

【０１２１】なお、関数ｆの具体例としては、数式６に示すものがある。

【数６】ｆ（ａ，ｂ）　＝　ａ　ＸＯＲ　ｂ

（ＸＯＲは排他的論理和）

この場合、ｆ　＝　ｆｉｎｖである。

【０１２２】第２のチケット鍵生成後、前記利用法Ｕの利用秘密情報を生成する。前段で生成された暗号化著作物データの復号鍵Ｋを前記真のチケット鍵Ｒを用いて、暗号化手段１５１により暗号化し、当該利用法の利用秘密情報を得る（ステップＡ’４－３）。

【０１２３】以上のようにして生成された第２のチケット鍵は、第１の実施の形態と同様に、利用条件記述中に埋め込まれ（ステップＡ’５）、チケットサーバ装置２に登録される（ステップＡ’６）。

【０１２４】一方、前記利用秘密情報から第１の実施の形態と同様に、前記アクセス制御テーブルが生成される。さらに、前記第２のチケット鍵の他に、前記第１の

チケットが必要となることを示すよう、チケット発行元リストが生成される。当該アクセス制御テーブルと当該チケットリストなどの著作物情報と前記暗号化著作物データとを含めて連結され、図２０に示すような構造をもつ第２のカプセル化著作物が生成され（ステップA’７）、流通センタ装置３に登録される（ステップA’８）。

【０１２５】次に、図１６のステップC’の処理について、図１７を参照して詳細に説明する。利用者は、利用法Uにより当該著作物を利用を要求する（ステップC’１）。そして、当該著作物の著作物情報から、前記チケットリストを参照し、必要となるチケットを判定する（ステップC’２）。

【０１２６】まず、チケットインターフェース部４４で、前記第２のチケットをチケットサーバ装置２に要求する（ステップC’３）。

【０１２７】当該要求を受けたチケットサーバ装置２は、第１の実施の形態と同様に、第２の著作物についての利用条件記述に、当該要求が合致するかどうかを判定し、合致すれば、第２のチケット鍵を生成し、第２の視聴装置７に送信する（ステップC’４）。

【０１２８】次に、同様にして、第２の視聴装置７は、前記第１のチケットをチケットサーバ装置２に要求し（ステップC’５）、チケットサーバ装置２は、条件判定した上で当該チケットを送信する（ステップC’６）。

【０１２９】こうして受信した第１および第２のチケットは、視聴装置７のカプセル化解除部４８で、前記カプセル化著作物より著作物データを復元するために、鍵統合手段７８２で、当該第１および第２のチケットから前記第１のチケット鍵Ｋ１および第２のチケット鍵Ｋ２を抽出し、数式７の計算を行う（ステップC’７）。

【数７】R’　＝　ｆｉｎｖ（Ｋ１，Ｋ２）

【０１３０】このとき、前記真のチケット鍵Rについて、数式８が成り立つ。

【数８】R’　＝　R

【０１３１】そして、復号手段４８１は、R’と前記利用秘密情報テーブル中の利用法Uに対応する利用秘密情報とを用いて、前記暗号化著作物データの復号鍵Kを復元する（ステップC’８）。

【０１３２】その後、復号手段４８１は、当該復号鍵Kと当該暗号化著作物データとを用いて、再び前記第２の著作物データを復元する（ステップC’９）。

【０１３３】本実施の形態では、二次的著作物の流通について、当該著作物に関する一次著作者および二次著作者の発行するチケットが同時に必要となるため、二次的著作物の著作権保護がより強固なものとなる。さらに、一般に巨大なサイズをもつ暗号化著作物データの復号処理は、この場合においても、１回のみであり、再生処理のスループット低下を最小限に抑えることができる。

【０１３４】［第３の実施の形態］図２１を参照すると、編集装置８が、図１に示された第１の実施の形態における編集装置１の構成に加え、課金モジュール編集部８７と、課金モジュール蓄積部８８とを有する点で異なる。また、視聴装置９が、図１に示された第１の実施の形態における視聴装置４の構成に加え、課金処理部９８と課金モジュール蓄積部９９とを有する点で異なる。さらに、電子財布装置１０１および決済サーバ装置１１１が図１に示された第１の実施の形態の構成に加えられている点で異なる。

【０１３５】課金モジュール編集部８７では、課金モジュールのソースコードを編集し、その実行形式を生成する。

【０１３６】課金モジュール蓄積部８８では、前段で作成された課金モジュールの実行形式を蓄積する。

【０１３７】課金処理部９８は、実行キュー管理手段９８１と、課金モジュール実行手段９８２とを備え、課金モジュール蓄積部９９に蓄積された課金モジュールの実行を行う。

【０１３８】課金モジュール蓄積部９９は、カプセル化著作物に同梱された課金モジュールを蓄積する。

【０１３９】電子財布装置１０１は、視聴装置９で発生した課金額を、決済予定金として記録し、定期的に決済サーバ装置１１１と決済処理のための通信を行う。

【０１４０】決済サーバ装置１１１は、電子財布装置１０１との通信により、決済情報を所定の金融機関に送信し、販売者または著作者への適切な振込処理を行う。

【０１４１】なお、図２１の著作物流通システムにおいて、電子財布装置１０１と決済サーバ装置１１１とは、視聴装置９と同一のコンピュータ装置上に実現することも可能である。

【０１４２】以下、本実施の形態の動作について、説明する。

【０１４３】まず、本実施の形態の動作全体の概略について、図２２を参照して説明する。著作者は、第１の実施の形態と同様に、著作物データの編集して登録し、また、利用条件を設定する。さらに、ここでは、課金方法と課金額も設定する（ステップA’’）。

【０１４４】次に、利用者は、視聴装置９で、カプセル化著作物インターフェース部により、前記カプセル化著作物を取得する（ステップB‘１）。取得後、カプセル化著作物インターフェース部４６は、当該カプセル化著作物から課金モジュールを抽出し、課金モジュール蓄積部９９に蓄積する。課金モジュールが除かれたカプセル化著作物は、カプセル化著作物蓄積部４７に蓄積される（ステップB’２）。

【０１４５】利用者は、その著作物について利用要求を行い、当該著作物のチケットをチケットサーバ装置２から取得して視聴装置４に蓄積する。さらに、ここでは、カプセル化著作物に対する課金処理も実行する（ステッ

ブC’’）。そして、再生処理部４３は、第１の実施の形態と同様に、著作物データの再生処理を行い、利用者による利用を可能にする（ステップD）。

【０１４６】次に、図２２のステップA’’の処理について、図２３を参照して詳細に説明する。著作者は、第１の実施の形態と同様に、編集装置８で、著作物データを作成する（ステップA’’１）。次に、当該著作物データに対して利用条件設定部１３で、各利用法ごとの利用条件を設定する。この際、第１の実施の形態における利用条件設定に加え、課金方法と課金額を設定するため、課金モジュール蓄積部８８に蓄積された課金モジュールの中から適当なものを選択する。もし、適当な課金モジュールがなければ、課金モジュール編集部８７で、新規な課金モジュールを作成し、使用することができる。そして、課金額や課金方法の詳細なパラメータなどを設定する。当該設定内容は、当該課金モジュールへの引数の形に変換される（ステップA’’２）。

【０１４７】次に、カプセル化処理部１５で、前記著作物データの暗号化が行われる（ステップA’’３）。そして、前記のように各利用法ごとに設定された課金モジュールについて、それぞれの実行形式を含む、一つの課金モジュールアーカイブが生成される（ステップA’’４）。そして、第１の実施の形態におけるカプセル化処理部１５の動作と同様に、チケット鍵および利用秘密情報が生成され（ステップA’’５）、前記暗号化著作物データと、利用秘密情報テーブルと、その他著作物情報と、前記課金モジュールアーカイブとから、図２５に示したような構造をもつカプセル化著作物が生成され（ステップA’’６）、流通センタ装置３に登録される（ステップA’’７）。

【０１４８】一方、前記課金モジュールの名前とその引数は、前記チケット鍵と同様に、利用条件記述中に埋め込まれ（ステップA’’８）、登録インターフェース部１６を介して、チケットサーバ装置２に登録される（ステップA’’９）。

【０１４９】次に、図２２のステップC’’の処理について、図２４を参照して詳細に説明する。当該カプセル化著作物の利用が行われる際、まず必要となるチケットが既に取得済みであるかどうかを判定し（ステップC’’１）、未取得であった場合、第１の実施の形態における視聴装置４と同様にして、チケットサーバ装置２よりチケットを取得し、蓄積する（ステップC’’２～C’’７）。既に当該チケットが取得済みであった場合、蓄積されたチケットにより、著作物データの復元処理へ進む。

【０１５０】ここで、当該チケットには、第１の実施の形態におけるチケットの記述（著作物ＩＤや著作者ＩＤなど）に加えて、前記課金モジュール名と、課金額などの当該課金モジュールへの引数に関する記述が、課金情報として、課金情報フィールドの中に含まれている（図２６）。

【０１５１】さらに、視聴装置９は、カプセル化解除部４８で、前記チケットを用いて、カプセル化著作物を、第１の実施の形態における視聴装置４と同様にして、当該カプセル化著作物に含まれるデータを分割する（ステップC’８）。

【０１５２】その後、視聴装置９、チケット中の課金情報フィールドを参照し、その内容を課金処理部９８に伝える。課金処理部９８では、当該課金情報を、実行キュー管理手段９８１に記録する（ステップC’’９）。実行キュー管理手段では、図２７に示されるように、チケットシリアル番号と、課金モジュール名と、課金額やその他の当該課金モジュールへの引数とが、テーブルの形で保持される。以下、このテーブルを実行キューと呼ぶ。

【０１５３】次に、課金処理部９８は、前記実行キューに登録された当該チケットに対応する課金モジュールを、課金モジュール蓄積部９９より抽出し、課金モジュール実行手段９８２で実行し、課金処理を行う（ステップC’’１０）。

【０１５４】課金モジュールは、課金方法を記述したプログラムであり、利用時に指定の課金額を収め、繰り返し同じ利用法による利用が可能となる一括方式や、回数に関わらず利用時に一定の課金額を収める必要のあるペイ・バー・ビュー方式などといった課金方法を記述できる。視聴装置９で、プログラムの内容に関わらず、一定の呼び出し規約により、課金処理を行うことができるように、図２８に示したような基本メソッドが、著作者もしくは販売者により定義されていることが規定されている。また、視聴装置９が有する各部を駆動するための手続きが、組込メソッドとして予め定義されており、課金モジュール内部で当該組込メソッドを呼び出すことにより、電子財布装置１０１へ課金情報を渡すなどといった処理を行うことができる。また、その他著作者に任意により定義されたユーザ定義メソッドも使用できる。基本メソッドの定義では、これら組込メソッドとユーザ定義メソッドを、適当に組み合わせて呼び出すことにより、様々な課金処理を行うことができる（図２９）。

【０１５５】課金モジュールによる具体的な課金処理の例を示す。まず、課金モジュールは、ｃｈａｒｇｅ（）という基本メソッドを必ず備えており、課金モジュール実行手段９８２はモジュールの種類によらずｃｈａｒｇｅ（）メソッドに、前記基本メソッドの引数（課金額および対応チケット、その他の情報）とともに、呼び出すことにより、課金処理を実行できるようにプログラムされている。そして、ｃｈａｒｇｅ（）メソッドが呼ばれると、引数として受け取った課金額とその振込先に関する情報を電子財布装置１０１に伝える。電子財布装置１０１では、前記課金額情報を保持し、一定時間間隔（例えば１日）で、決済サーバ装置１１１と通信して、決済

処理を行う。決済サーバ装置１０では、前記振込先に対して前記課金額を振り込むための処理を行う。

【０１５６】また、必要に応じて、もう一つの基本メソッドであるｅｘｐｉｒｅ（）が呼び出される。ｅｘｐｉｒｅ（）メソッドの実行により、前記実行キューからの当該課金モジュールの削除が行われる。さらに、ｄｉｓａｂｌｅ＿ｔｉｃｋｅｔ（）が呼び出されると、前記対応チケットの無効化が行われる。無効化されたチケットは、それ以降の著作物の利用時に、視聴装置９で通常のチケットとして扱われることはない。また、ｔｒａｎｓｍｉｔＴｏＷａｌｌｅｔ（）が呼び出されると、引数に示された額が決済予定金として、電子財布装置９に記録される。

【０１５７】課金モジュールの具体的な構成例としては、最初のｃｈａｒｇｅ（）メソッド呼出しで、ｅｘｐｉｒｅ（）メソッドとｄｉｓａｂｌｅ＿ｔｉｃｋｅｔ（）メソッドが呼び出されると、いわゆるペイ・パー・ビュー方式の課金が実現できる。また、最初のｃｈａｒｇｅ（）メソッド呼出しで、ｅｘｐｉｒｅ（）メソッドのみが呼び出された場合、従来の購入方式（商品の受取時に対価を支払う）が実現される。さらに、購入日時と利用可能期間をｃｈａｒｇｅ（）メソッドへの引数として呼び出し、当該購入日時から当該利用可能期間を経た日時にｅｘｐｉｒｅ（）メソッドおよびｄｉｓａｂｌｅ＿ｔｉｃｋｅｔ（）メソッドが呼び出された場合、ビデオレンタルなどのような時限付課金方式が実現できる。

【０１５８】本実施の形態では、適切な課金モジュールの適用により、著作者や販売者の意向と、著作物の性格などにより、効果的な課金方法の選択が柔軟にできるようになる。さらに、課金処理と決済処理を２段階に分けて行い、電子財布装置１００と決済サーバ装置１０１との間の通信にはＳＥＴなど従来の電子決済方式が適用できるため、既存の決済機構との親和性にも優れている。

【０１５９】［実施の形態の変形］本発明は、上記の実施の形態に限られず、種々の変形、応用が可能である。以下、本発明に適用可能な上記の実施の形態の変形態様について、説明する。

【０１６０】上記の第１の実施の形態において、編集装置１で生成したカプセル化著作物を、登録インターフェース部１６を介して流通センタ装置３へ登録することなく、書き込み可能なコンパクトディスクなどの不揮発性メモリにカプセル化著作物を書き出してもよい。この選択は、著作者の任意による。そして、視聴装置４でカプセル化著作物を取得する場合、流通センタ装置３にアクセスするのではなく、上記不揮発性メモリを取得し、カプセル化著作物蓄積部４４で当該不揮発性メモリをアクセスできるようにする。この場合は、当該不揮発性メモリを店舗に置くなどの物理世界での流通が可能となり、著作物データのサイズが非常に大きくなり、ネットワーク上を流通させることが困難な場合にも対応できる。

【０１６１】上記の第２の実施の形態において、鍵分割手段６５４は、鍵分割関数として、前記真のチケット鍵Ｒを鍵とする共有鍵暗号を用いて一次著作者のチケット鍵Ｋ１から二次著作者のチケット鍵Ｋ２を生成することもできる。この場合、鍵統合手段７８２では、チケット鍵Ｋ２を鍵として前記共有鍵暗号によりＫ１からＲを復元する。もっとも、第ｎ次著作物（ｎ＞２）のチケット鍵生成には、前記のように共有鍵暗号をもちいた鍵分割を行うことはできない。

【０１６２】その点、前記鍵分割関数ｆを用いることで、このような第三次以降の著作物のチケット鍵生成が可能になる。この場合、ｎ次著作者は、第一次～第（ｎ－１）次著作者のチケット鍵Ｋ１～Ｋｎ－１を取得し、真のチケット鍵Ｒを乱数により生成し、鍵分割手段６５４で、前記鍵分割関数ｆに対して、数式９を計算する。

【数９】Ｋｎ　＝　ｆ（Ｋ１，　Ｋ２，．．．，　Ｋｎ－１，　Ｒ）

【０１６３】また、鍵統合手段７８２では、前記と同様にして、次の数式１０を計算して、真のチケット鍵Ｒを復元する。

【数１０】Ｒ　＝　ｆｉｎｖ（Ｋ１，　Ｋ２，．．．，　Ｋｎ－１，　Ｋｎ）

こうした場合、第（ｎ－１）次著作者までのチケット鍵Ｋ１～Ｋｎ－１の取得順序は任意でよい。

【０１６４】上記の第１～第３の実施の形態では、チケット鍵には、暗号と復号とで共通の鍵を使用する対称鍵暗号系を用いていた。これに対し、チケット鍵には、暗号と復号とで別の鍵が用いられる非対称鍵暗号系を用いてもよい。

【０１６５】上記の第１～第３の実施の形態では、編集装置１、６、８と、チケットサーバ装置２と、流通センタ装置３とは、それぞれ別個のコンピュータ装置上で実現され、ネットワークで接続されるものとしていた。しかしながら、これらのすべて或いはそのうちの任意の２つを、同一のコンピュータ装置上で実現することも可能である。

【０１６６】上記の第１～第３の実施の形態では、編集装置１、６、８、チケットサーバ装置２、流通センタ装置３、（第１、第２を含む）視聴装置４、５、７、９には、それぞれ各部、手段の機能が実現されているものとしていた。これに対し、これらの機能を実現するためのプログラムは、ＣＤ－ＲＯＭやフロッピーディスクなどのコンピュータ読み取り可能な記録媒体に格納して配布してもよい。

【０１６７】

【発明の効果】以上説明したように、本発明によれば、配信されるカプセル化著作物にはその著作物データの復号鍵が含まれていないため、著作物データを自由に配布することが可能となる。そして、著作物データを利用さ

せる場合には、チケット配信手段からチケット復号鍵を配信するだけでよく、著作物の流通範囲の拡大と利用促進を望めるようになる。

【０１６８】また、著作物データの利用条件毎に異なるチケット鍵（暗号鍵及び復号鍵）が生成することができる。このため、著作者及び販売者の意図を反映させて、利用条件を設定し、著作物データを利用させることができる。

【０１６９】さらに、二次著作物データを生成し、生成された二次著作物データを配布すべき著作物データとすることで、一次著作物データと同様に流通させることができるので、著作活動の活性化が可能となる。また、その基となる著作物データのチケット復号鍵も必要となるので、一次著作者の権利保護を十分に図ることができる。

【０１７０】さらに、課金モジュールを利用条件毎に生成し、課金処理を課金モジュールで行うことにより、著作者や販売者の意図、或いは著作物の性格などに従って、適切な課金方法を柔軟に選択することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態の著作物流通システムの構成を示すブロック図である。

【図２】本発明の第１の実施の形態の動作の概略を示す流れ図である。

【図３】本発明の第１の実施の形態における編集装置の動作を示す流れ図である。

【図４】本発明の第１の実施の形態における流通センタ装置と視聴装置との通信動作を示す流れ図である。

【図５】本発明の第１の実施の形態におけるチケットサーバ装置と視聴装置との通信動作を示す流れ図である。

【図６】利用条件設定ダイアログの一例である。

【図７】利用条件設定操作の一例である。

【図８】チケット鍵生成動作を示す図である。

【図９】利用秘密情報テーブルの一例である。

【図１０】本発明の第１の実施の形態におけるカプセル化著作物の構造の一例である。

【図１１】利用条件記述の構造と、アクセス制御言語による利用条件記述の一例である。

【図１２】著作物が複数オブジェクトから構成される場合の階層構造の一例と、そのアクセス制御言語による利用条件記述の一例である。

【図１３】流通センタ装置にアクセスした際、視聴装置で表示される著作物インデックス画面の一例である。

【図１４】本発明の第１の実施の形態におけるチケットの構造の一例である。

【図１５】本発明の第２の実施の形態の著作物流通システム構成を示すブロック図である。

【図１６】本発明の第２の実施の形態の動作の概略を示す流れ図である。

【図１７】本発明の第２の実施の形態における第１の視聴装置および編集装置の動作を示す流れ図である。

【図１８】本発明の第２の実施の形態におけるチケットサーバ装置と第２の視聴装置との通信動作を示す流れ図である。

【図１９】分割関数を用いた第２のチケット鍵生成を示す図である。

【図２０】本発明の第２の実施の形態におけるカプセル化著作物の構造の一例である。

【図２１】本発明の第３の実施の形態の著作物流通システムの構成を示すブロック図である。

【図２２】本発明の第３の実施の形態の動作の概略を示す流れ図である。

【図２３】本発明の第３の実施の形態における編集装置における動作を示す流れ図である。

【図２４】本発明の第３の実施の形態におけるチケットサーバ装置と視聴装置との通信動作を示す流れ図である。

【図２５】本発明の第３の実施の形態におけるカプセル化著作物の構造の一例である。

【図２６】本発明の第３の実施の形態におけるチケットの構造の一例である。

【図２７】実行キューの一例である。

【図２８】課金モジュールにおけるメソッド種別と、各メソッドの機能の一例である。

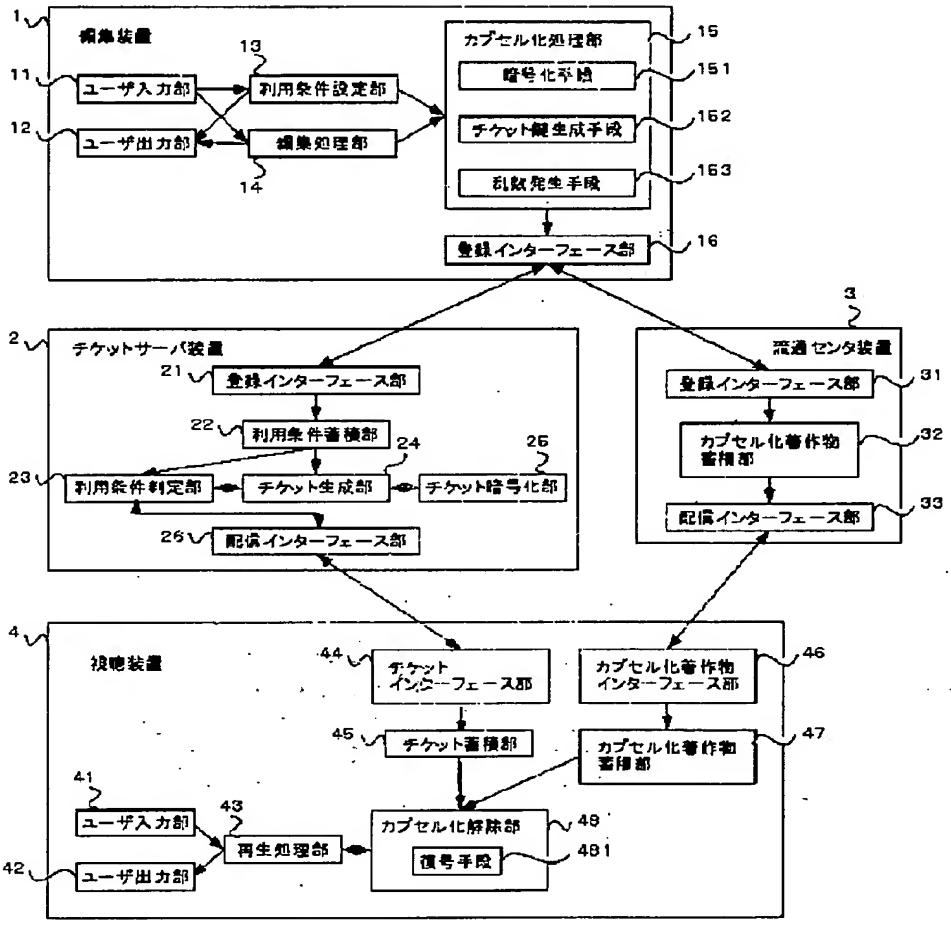
【図２９】課金モジュールの構造と、その具体例を示す図である。

【符号の説明】

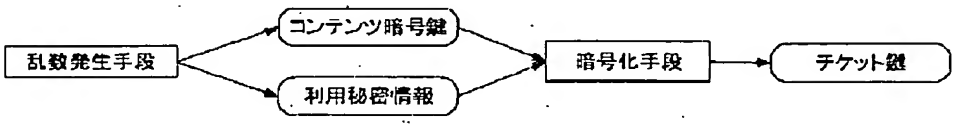
１	編集装置
１１	ユーザ入力部
１２	ユーザ出力部
１３	利用条件設定部
１４	編集処理部
１５	カプセル化処理部
１５１	暗号化手段
１５２	チケット鍵生成手段
１５３	乱数発生手段
１６	登録インターフェース部
２	チケットサーバ装置
２１	登録インターフェース部
２２	利用条件蓄積部
２３	利用条件判定部
２４	チケット生成部
２５	チケット暗号化部
２６	配信インターフェース部
３	流通センタ装置
３１	登録インターフェース部
３２	カプセル化著作物蓄積部
３２	配信インターフェース部
４	視聴装置
４１	ユーザ入力部

４２　ユーザ出力部
４３　再生処理部
４４　チケットインターフェース部
４５　チケット蓄積部
４６　カプセル化著作物インターフェース部
４７　カプセル化著作物蓄積部
４８　カプセル化解除部
４８１　復号手段
５　視聴装置
６　編集装置
６５３　鍵分割手段
７　視聴装置
＊７８２　鍵統合手段
８　編集装置
８７　課金モジュール編集部
８８　課金モジュール蓄積部
９　視聴装置
９８　課金処理部
９８１　実行キュー管理手段
９８２　課金モジュール実行手段
９９　課金モジュール蓄積部
１０１　電子財布装置
１１１　決済サーバ装置
＊

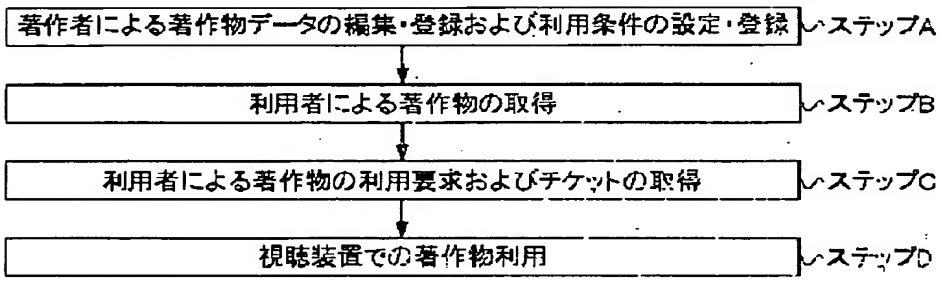
【図１】



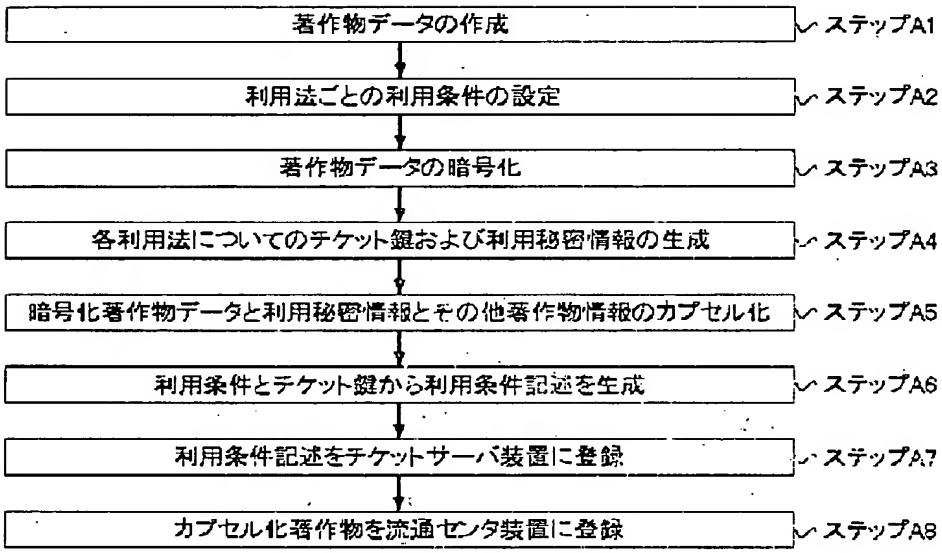
【図８】



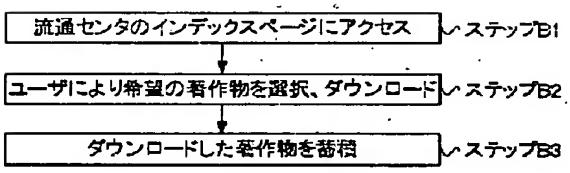
【図２】


著作者による著作物データの編集・登録および利用条件の設定・登録
ステップA
利用者による著作物の取得
ステップB
利用者による著作物の利用要求およびチケットの取得
ステップC
視聴装置での著作物利用
ステップD

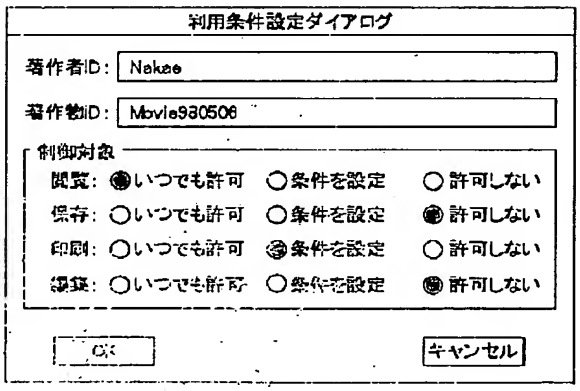
【図３】


著作物データの作成
ステップA1
利用法ごとの利用条件の設定
ステップA2
著作物データの暗号化
ステップA3
各利用法についてのチケット鍵および利用秘密情報の生成
ステップA4
暗号化著作物データと利用秘密情報とその他著作物情報のカプセル化
ステップA5
利用条件とチケット鍵から利用条件記述を生成
ステップA6
利用条件記述をチケットサーバ装置に登録
ステップA7
カプセル化著作物を流通センタ装置に登録
ステップA8

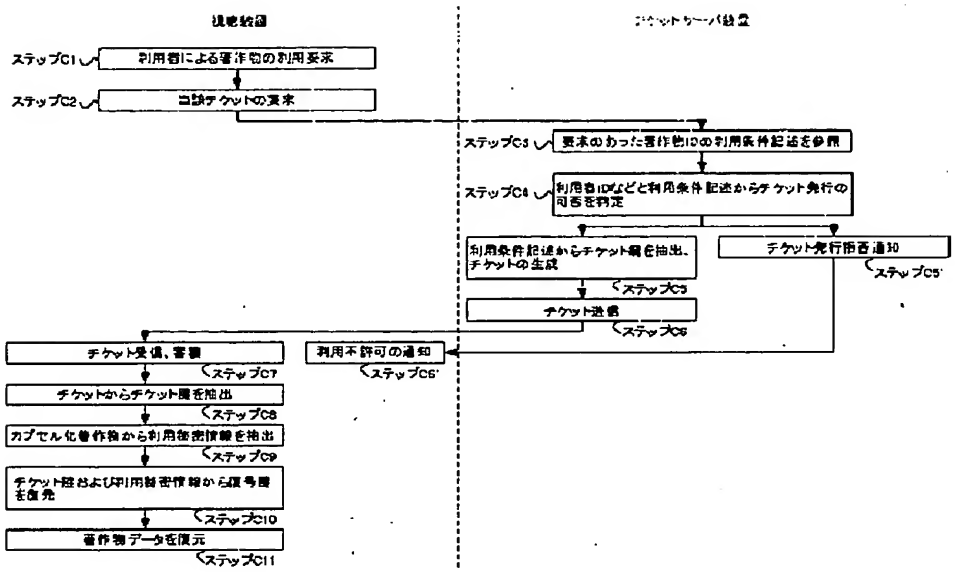
【図４】


流通センタのインデックスページにアクセス
ステップB1
ユーザにより希望の著作物を選択、ダウンロード
ステップB2
ダウンロードした著作物を蓄積
ステップB3

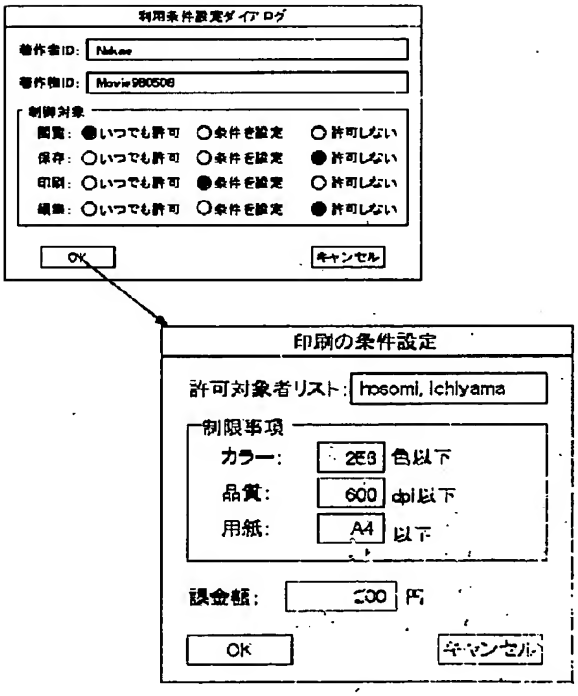
【図６】


利用条件設定ダイアログ
著作者ID: Nakae
著作物ID: Movie980506
制御対象
閲覧: いつでも許可 条件を設定 許可しない
保存: いつでも許可 条件を設定 許可しない
印刷: いつでも許可 条件を設定 許可しない
編集: いつでも許可 条件を設定 許可しない
OK
キャンセル

【図５】



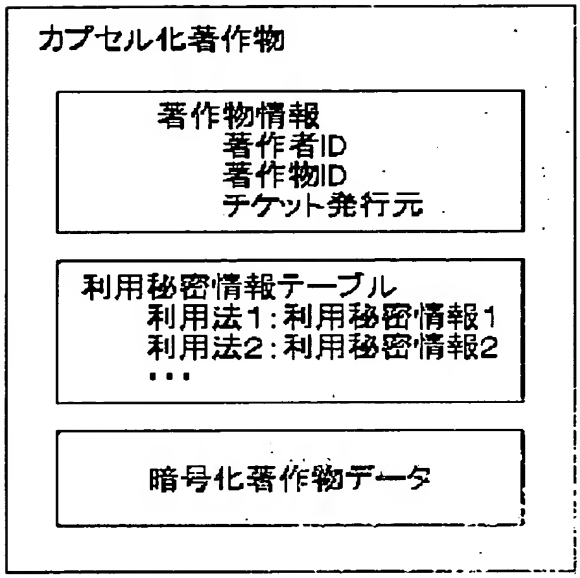
【図７】



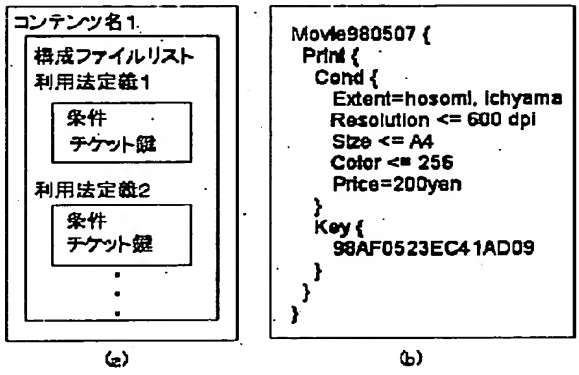
【図９】

利用法	秘密情報
閲覧	95AD438A
保存	N/A
印刷	F38F05AD
編集	N/A

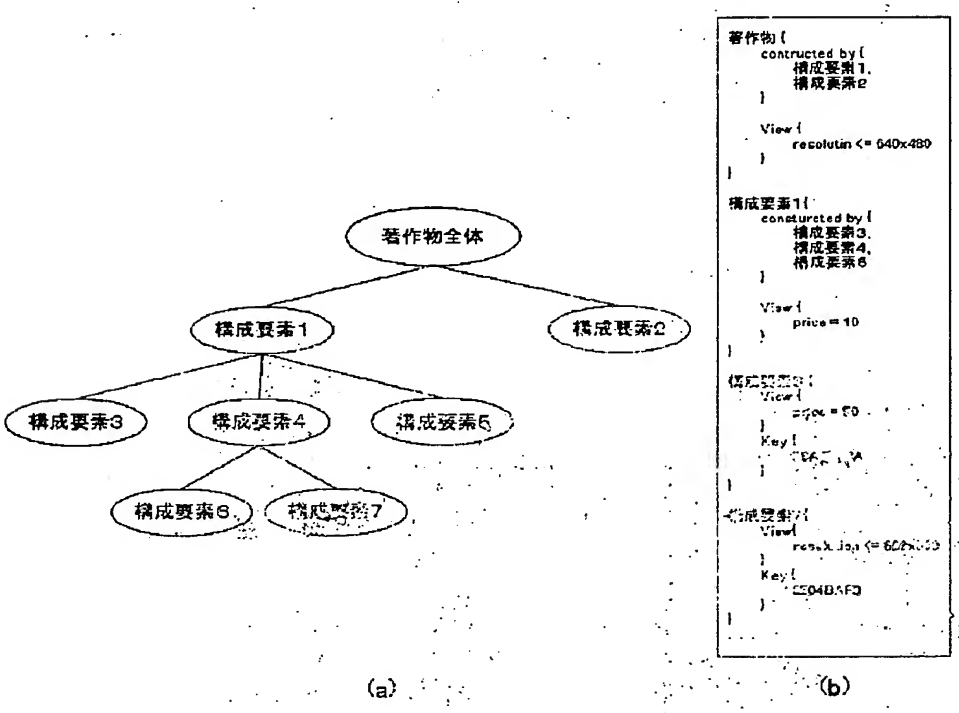
【図10】


カプセル化著作物
著作物情報
著作者ID
著作物ID
チケット発行元
利用秘密情報テーブル
利用法1：利用秘密情報1
利用法2：利用秘密情報2
・・・
暗号化著作物データ

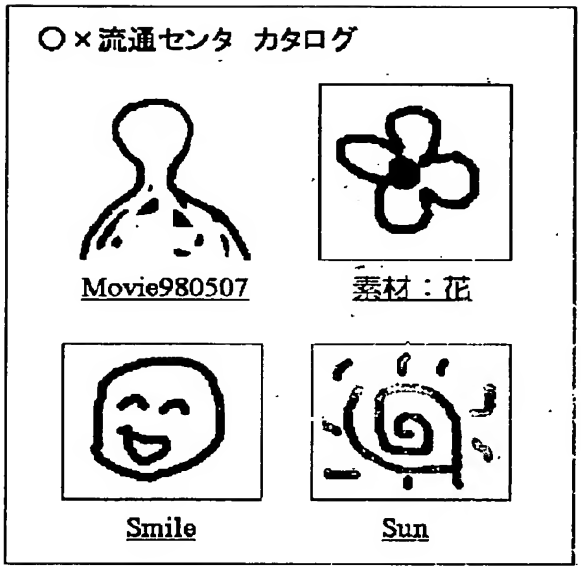
【図11】


コンテンツ名1
構成ファイルリスト
利用法定義1
条件
チケット鍵
利用法定義2
条件
チケット鍵
Movie980507 {
Print {
Cond {
Extent=hosomi, ichyama
Resolution <= 600 dpi
Size <= A4
Color <= 256
Price=200yen
}
Key {
98AF0523EC41AD09
}
}
}
(a)
(b)

【図12】


著作物全体
構成要素1
構成要素2
構成要素3
構成要素4
構成要素5
構成要素6
構成要素7
著作物 {
contructed by {
構成要素1,
構成要素2
}
View {
resolutin <= 640x480
}
}
構成要素1 {
contructed by {
構成要素3,
構成要素4,
構成要素6
}
View {
price = 10
}
}
Key {
}
(a)
(b)

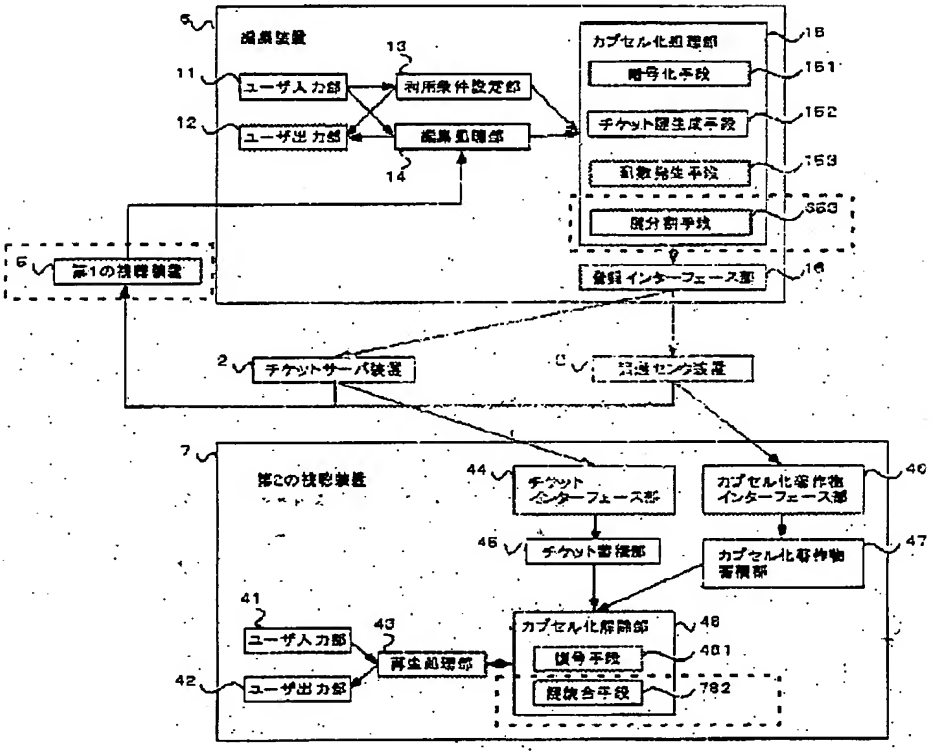
【図１３】



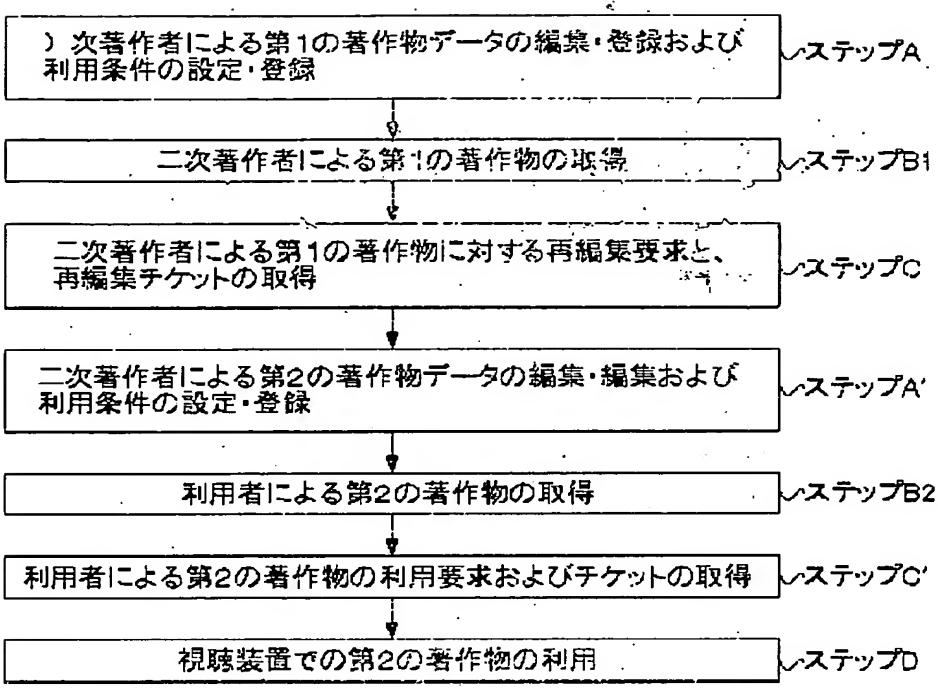
【図１４】

著作物ID	Movie980507
利用者ID	nakae
チケットシリアル番号	TK980507.AZK8311
チケット鍵	98AF0523EC41AD09
許可された利用法	Print
発行年月日	1998/05/07
有効期限	1999/05/07

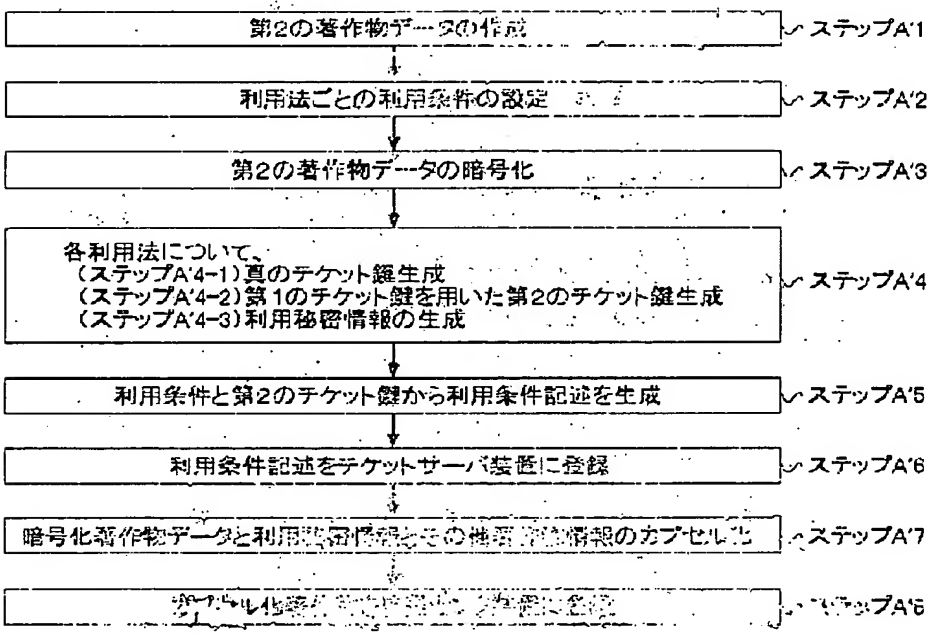
【図１５】



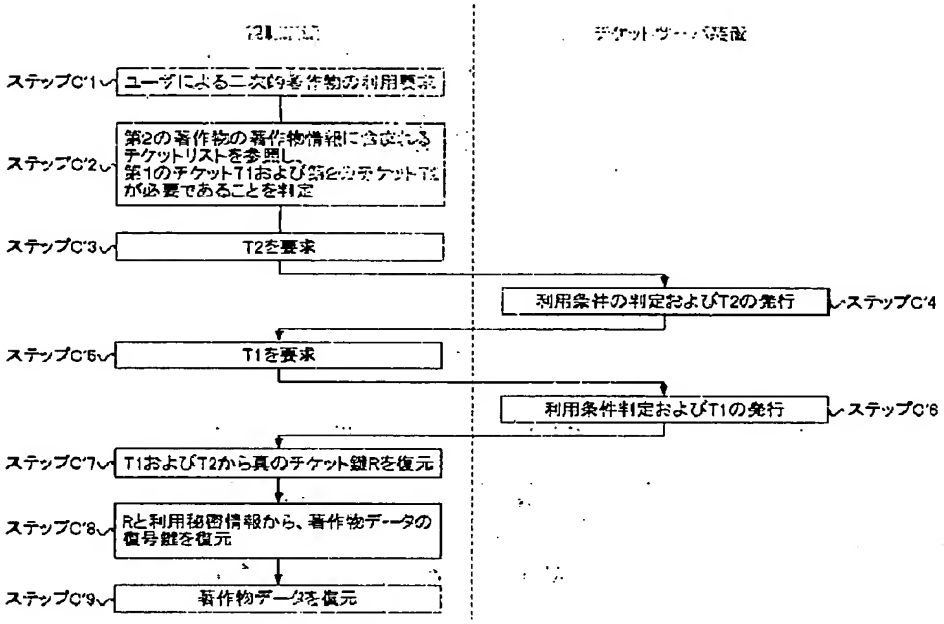
【図１６】


）次著作者による第1の著作物データの編集・登録および利用条件の設定・登録
ステップA
二次著作者による第1の著作物の取得
ステップB1
二次著作者による第1の著作物に対する再編集要求と、再編集チケットの取得
ステップC
二次著作者による第2の著作物データの編集・編集および利用条件の設定・登録
ステップA'
利用者による第2の著作物の取得
ステップB2
利用者による第2の著作物の利用要求およびチケットの取得
ステップC'
視聴装置での第2の著作物の利用
ステップD

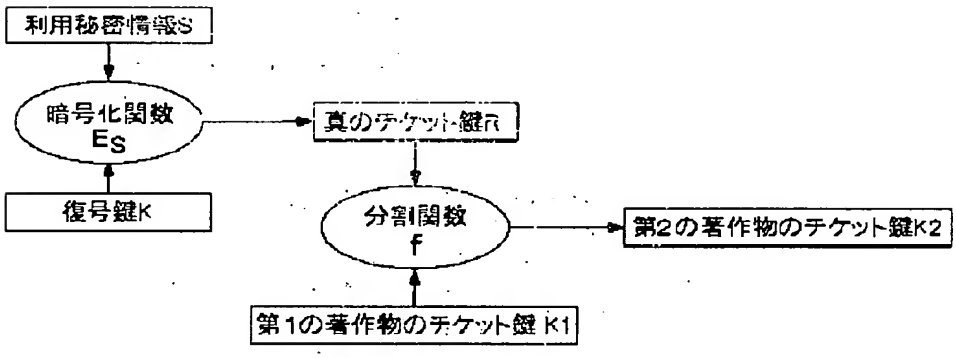
【図１７】


第2の著作物データの作成
ステップA'1
利用法ごとの利用条件の設定
ステップA'2
第2の著作物データの暗号化
ステップA'3
各利用法について、
（ステップA'4-1）真のチケット鍵生成
（ステップA'4-2）第1のチケット鍵を用いた第2のチケット鍵生成
（ステップA'4-3）利用秘密情報の生成
ステップA'4
利用条件と第2のチケット鍵から利用条件記述を生成
ステップA'5
利用条件記述をチケットサーバ装置に登録
ステップA'6
暗号化著作物データと利用秘密情報とその他の情報のカプセル化
ステップA'7
ステップA'8

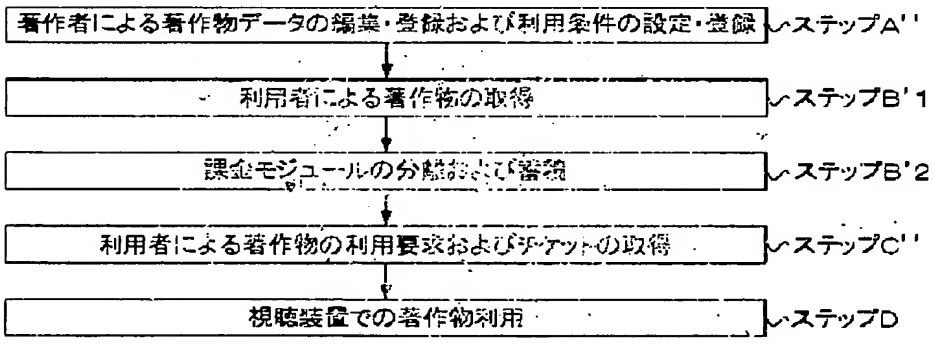
【図１８】


ステップC'1
ユーザによる二次的著作物の利用要求
ステップC'2
第2の著作物の著作物情報に含まれるチケットリストを参照し、第1のチケットT1および第2のチケットT2が必要であることを判定
ステップC'3
T2を要求
利用条件の判定およびT2の発行
ステップC'4
ステップC'5
T1を要求
利用条件判定およびT1の発行
ステップC'6
ステップC'7
T1およびT2から真のチケット鍵Rを復元
ステップC'8
Rと利用秘密情報から、著作物データの復号鍵を復元
ステップC'9
著作物データを復元

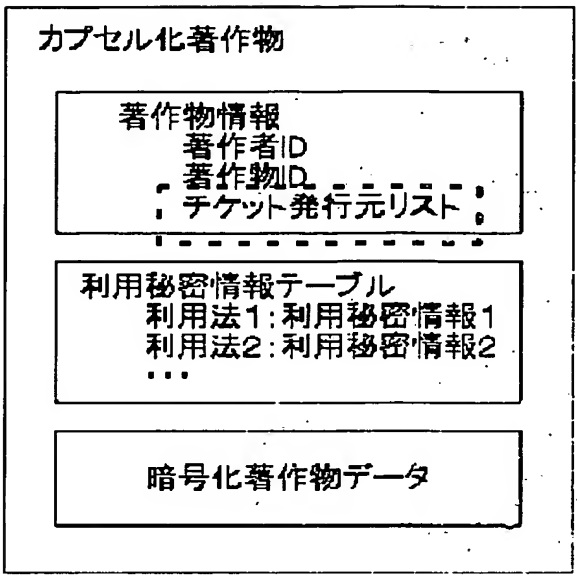
【図１９】


利用秘密情報S
暗号化関数
Es
復号鍵K
真のチケット鍵R
分割関数
f
第2の著作物のチケット鍵K2
第1の著作物のチケット鍵 K1

【図２２】


著作者による著作物データの編集・登録および利用条件の設定・登録
ステップA''
利用者による著作物の取得
ステップB'1
課金モジュールの分離および登録
ステップB'2
利用者による著作物の利用要求およびチケットの取得
ステップC''
視聴装置での著作物利用
ステップD

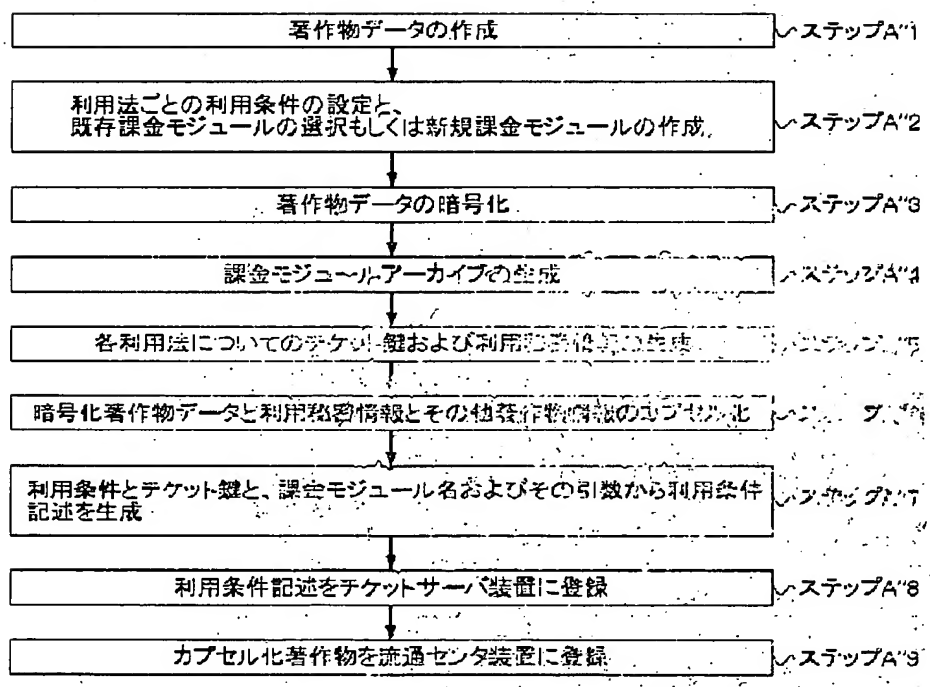
【図２０】



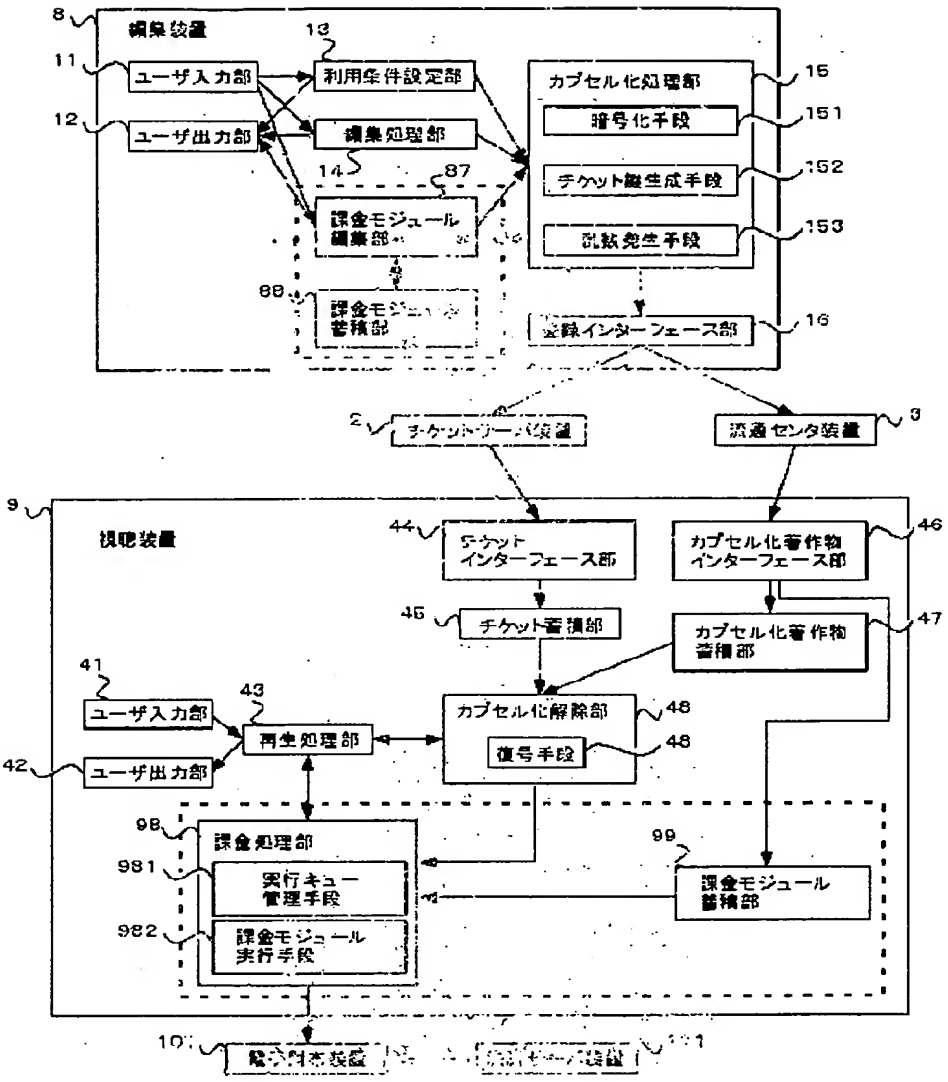
【図２６】

著作物ID	Movie980507
利用者ID	nakae
チケットシリアル番号	TK980507.AZK8311
チケット鍵	98AF0523EC41AD09
許可された利用法	Print
課金モジュール名	chargeAtOnce
課金モジュールへの引数	4,000yen
発行年月日	1998/05/07
有効期限	1999/05/07

【図２３】



【図２１】

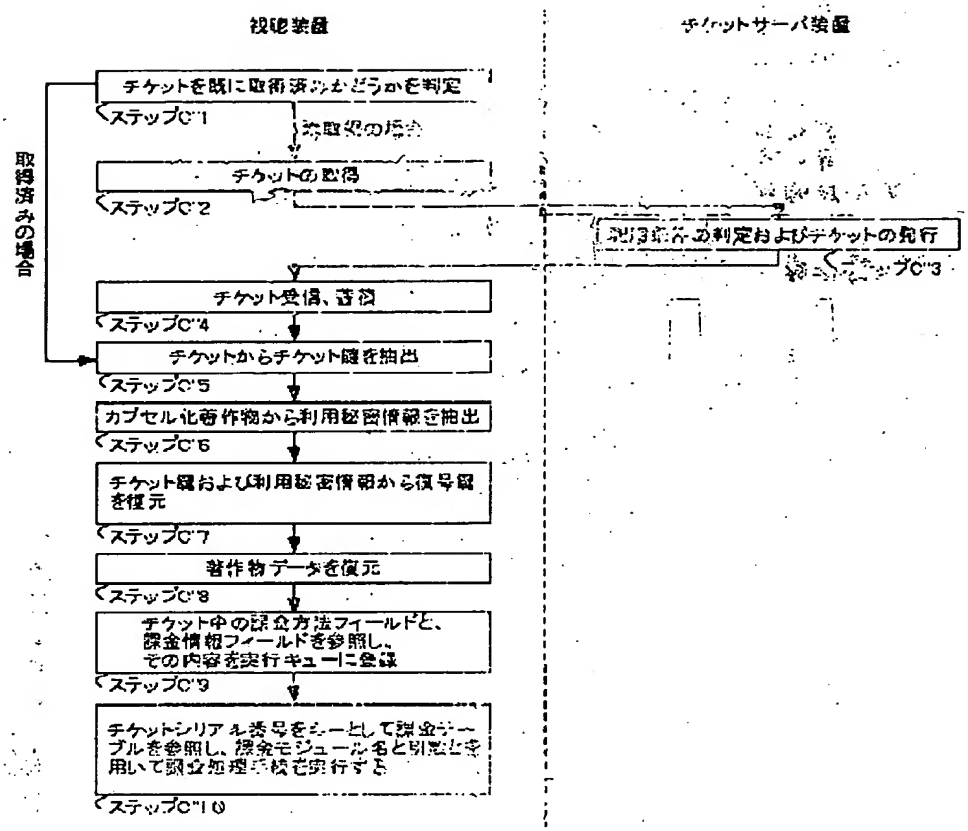


【図２７】

実行キュー

チケットシリアル番号	モジュール名	引数	モジュール呼出
TK980507.AZK8311	chargeAtOnce	4,000yen	→ chargeAtOnce("4000yen")
TK970120.FA15001	chargePerUse	50yen	→ chargePerUse("50yen")
TK980507.GBDA99	chargeTill	500yen, 12:00 Aug 18 1998	→ chargeTill("500yen", "12:00 Aug 18 1998")
...	...	...	

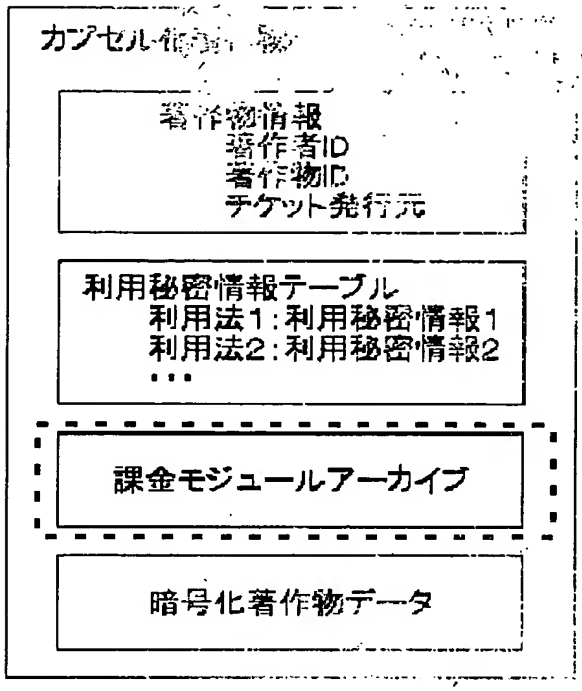
【図２４】



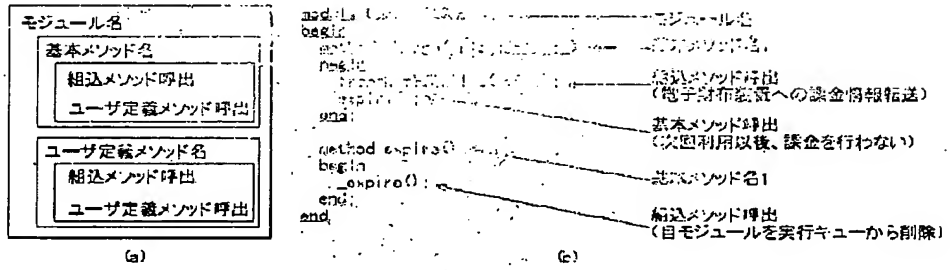
【図２３】

基本メソッド	charge()	課金処理を行う
	expire()	自課金モジュールを実行キューから削除し、それに伴う処理を行う
組込メソッド	disableTicket()	チケットの無効化を行う
	transmitToWallet()	課金情報を電子財布装置に送る
	timer()	定期的にcharge()を呼ぶよう設定を行う
	_expire()	内部に自課金モジュールを実行キューから削除
ユーザ定義メソッド	著作者により自由に定義	

【図２５】



【図３１】



フロントページの続き

(51)Int.Cl.'	識別記号	FI		テーマコード (参考)
H04L 9/08		H04L 9/00	601C	
9/32			601Z	
			675A	

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLORED OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning documents *will not* correct images problems checked, please do not report the problems to the IFW Image Problem Mailbox